

网管实战宝典

专业网管笔记　成就资深网管

网络安全大全

胡文启　徐军　张伍荣◎主编

PROFESSIONAL NETWORK MANAGEMENT
SENIOR NOTES ACHIEVEMENTS

清华大学出版社

网管实战宝典

网 络 安 全 大 全

胡文启　徐　军　张伍荣　主编

清华大学出版社
北　京

内 容 简 介

本书以“应用实例导航”为主线，由浅入深、系统全面地介绍了网络安全中所遇到的一些问题和常用的网络安全设备的使用方法。

本书以企业网络应用的安全需求作为出发点，以实例的形式陈述攻击行为，然后对攻击原理进行分析，并通过部署相应的设备防止攻击再次发生来介绍网络安全。本书结构清晰，易教易学，实例丰富，可操作性强，注重能力的提高，既可作为大中专院校的教材，也可作为各类培训班的培训教材。此外，本书也可作为各类企业网络管理员及各类网络爱好者、企业IT经理以及网络安全工程师的参考用书。

图书在版编目(CIP)数据

网络安全大全/胡文启，徐军，张伍荣主编. —北京：清华大学出版社，2008.10
(网管实战宝典)
ISBN 978-7-302-18619-9

Ⅰ. 网…　Ⅱ. ①胡…　②徐…　③张…　Ⅲ. 计算机网络—安全技术　Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2008)第144785号

责任编辑：章忆文　宣　颖
封面设计：柏拉图+创意机构
版式设计：北京东方人华科技有限公司
责任校对：李凤茹
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　**印　张**：26.25　**字　数**：620千字
版　次：2008年10月第1版　**印　次**：2008年10月第1次印刷
印　数：1~4000
定　价：39.80元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　产品编号：

丛　书　序

他山之石，可以攻玉。——《诗经》
你应该了解真相，真相会使你自由。——《圣经》
我之所以成功，是因为站在巨人的肩膀上。——牛顿

策划初衷

网管员(Network Administrator)是国家劳动和社会保障部近年颁布的第四批国家职业标准中明确规定的一个新兴职业。网管员职业要求从业者具备一系列专业、高端的计算机及网络操作技能。

为了给广大网管员提供一套标准实用的高效实战教材，清华大学出版社在广泛调研与充分论证的基础上，聘请了国内著名院校资深学者和实战经验丰富的网管专家，历时18个月精心打造了这套《网管实战宝典》。本丛书由网管员的职业应用切入，根据网管员的行业内容细划科目，以实际工作的项目案例为主线，解决实际应用中可能出现的问题，是目前市面上唯一从“网管员职业应用案例实战”角度切入的精品丛书。本套丛书全面介绍网络管理、设计与维护的热点应用案例，剖析透彻，确保技术的先进性、实用性和深入性，是网络管理员必备的实践读物。

首推书目

《网管实战宝典》系列首批推出9本，书目如下。

1.《中型局域网组建一本通》
2.《网络规划、设计与配置》
3.《Windows Server 2003 配置与管理》
4.《Windows Server 2003 服务器架设与管理》
5.《网络管理工具使用大全》
6.《网络安全大全》
7.《Linux 服务器架设与管理》
8.《网络故障排除与维护技巧》(Windows 版)
9.《网络故障排除与维护技巧》(Linux 版)

丛书特色

本丛书具有以下主要特色。

1. 针对性

从网管员职业应用切入，以网管员的行业内容细划科目，所介绍的内容紧紧围绕网管员必备的知识与技能展开，从而突出针对性。

2. 实用性

以实际的项目案例为主线，解决实际应用中可能出现的问题，而不仅仅是理论上的介绍。这些应用案例是广大专业人士多年的网管实战经验总结，对读者朋友有最直接、最宝贵的指导意义。

3. 可操作性

本丛书在介绍各种实际应用配置方案时，都以图解、截屏等方式与清晰的步骤相结合，避免泛泛而谈，并且着重强调了各步配置细节，方便读者按步骤操作，快速掌握案例操作过程。

4. 先进性

本丛书所介绍的各种网络技术和方案均是当前最主流，甚至最新的，读者通过阅读本丛书即可了解当前最主流，甚至最新的网络技术与应用方案。

5. 深入性

丛书中的应用案例讲解细致入微，分析透彻，过程完整，从而确保读者能够完全理解与掌握，以便在实际工作中应用与借鉴。

6. 精彩点拨

丛书以大量点评与拓展、注意、提示等特色段落为辅线，帮助读者理解与加深关键技术，使读者学得轻松，记得深刻，用得灵活。

读者对象

1. 从事网管员职业的人员。
2. 有志于网络管理员职业的读者。
3. 大专院校计算机相关专业师生，以及网络培训班学员。

创作团队

我们一直深信一流的团队，奉献一流的作品，成就一流的读者。本丛书创作团队来源

于著名院校资深学者、实战经验丰富的网管专家，他们长期工作于网管一线，有多年的网络管理与设计经历，经验丰富，实力雄厚。

互动交流

读者的进步，是我们的心愿。本丛书愿为读者提供全面的技术支持，服务方式包括：

(1) 技术讲座。将在适当的时间组织专家进行技术巡讲，介绍最新的技术并当面解答读者的疑问。

(2) 版本升级。本丛书将跟踪最新网络技术发展动态，及时更新版本，为读者提供最新的网络技术。

(3) 问题解答。如果您阅读本丛书的过程中，发现任何问题或疑问，或者有什么意见或建议，请发邮件至我们的答疑信箱 Book21Press@126.com，我们将及时为您提供解决方案。

特别致谢

在此，我们对丛书所选用的参考文献的著作者，以及丛书所引用网站及其他相关著作者表示真诚的感谢。感谢为本丛书出版提供帮助的各界人士。

知识是一个宝库，实践是打开这个宝库的钥匙。
借助于别人成功的实践经验，便是捷径。
我们乐意与您一同分享成功的网管实践经验。

——编委会

前　言

随着网络和信息技术的快速发展和日益普及，信息化成为现代企业生存的必要条件。随着企业内部信息化程度逐渐加深，网络管理员这一职业应运而生。能否管理好企业的网络事关企业的成败。

清华大学出版社策划出版了网管实战宝典系列丛书，本书是该系列教材之一。

1．关于网络安全

网络安全实现通常很难，而且实现的成本很高，在电子通信成为无处不在的通信手段的今天，电子商务等商业实践在企业网络基础设施上逐渐展开，各个企业都试图了解和控制与之相关的风险。企业网络安全变得越来越流行，同时也使得人们感到有些担忧。绝对安全的网络是不存在的，任何设备都有配置错误或者缺陷。因此网络安全是一个长期的过程，并且需要进行日常的风险审计和风险消除。本书就是基于这样的原则，以企业网络应用的安全需求作为出发点，以实例的形式陈述攻击行为，然后对攻击原理进行分析，并通过部署相应的设备防止攻击再次发生来介绍网络安全。同时也介绍了日常安全审计的要点，从而可有效地防止网络风险。

2．本书阅读指南

本书由浅入深、系统全面地介绍了网络安全中所遇到的一些常见问题和常用的网络安全设备使用方法。全书共分 13 章。

第 1 章主要介绍网络安全的基本原理。通过分析攻击事件的来源描述了网络安全的关键要素以及用户应具备的网络安全意识。同时讲述了一些常见的攻击实例，并对其进行了风险分析。

第 2 章主要介绍了防范常见网络攻击事件的一些方法和解决方案，并简要介绍了路由器、防火墙、VPN、IPS 等各种网络安全设备的使用。

第 3 章从几个不同的方面讨论网络设备的安全。首先是网络设备的物理安全，其中包括供电安全、环境安全等，然后介绍了各种网络设备的访问权限及相应的漏洞攻击和防范方法等；最后详细介绍了网络冗余的一些协议和实施方案。

第 4 章主要介绍路由器及路由协议安全，通过配置安全的路由协议和访问控制使得路由器更加安全。

第 5 章主要介绍交换网络安全，并介绍了处理广播攻击、MAC 攻击、VLAN 欺骗、ARP 病毒等二层攻击的方法。

第 6 章主要介绍 AAA 体系结构以及基于 Radius 的身份认证体系，同时也介绍了 Windows 电子证书服务及 PKI 证书体系。

第 7 章主要介绍网络安全接入以及终端安全，同时介绍了部署 802.1x、Cisco NAC 以及

WSUS 自动更新服务的配置方式。同时还介绍了基于终端的安全防护产品 CSA/CSA-MC。

第 8 章主要介绍防火墙的工作原理，同时介绍了 Cisco PIX/ASA 防火墙、微软 ISA 防火墙以及 Linux 防火墙的配置方式。

第 9 章主要介绍入侵检测系统和入侵防御系统的配置方式，并讲述了常见 IPS/IDS 系统及 IDS 的部署，最后介绍了基于 Cisco 的 DDoS 防御技术。

第 10 章主要介绍远程访问的知识，并且介绍了 IPSec VPN、SSL VPN、ISA Server VPN 和 Linux VPN 的配置方式，同时还介绍了常见的 VPDN 远程接入配置。

第 11 章主要介绍网络管理软件，如何通过对日志进行统一管理获得较快的攻击响应速度。

第 12 章主要介绍基于 EFS 的文件加密系统和 RMS 文件权限控制系统等。

第 13 章根据各种企业规模进行了网络安全方案设计，并根据企业的规模和资金状况设计了多种网络安全升级方案。

3. 本书特色与优点

(1) 系统地讲述了局域网面临的安全问题及防范措施。本书对局域网络中的关键软硬件设备，如操作系统、服务器、客户机、路由器、交换机和防火墙的安全性进行了分析，并针对这些设备的安全隐患指出了加固的方法，其目的是从整体上提高局域网络的安全防御能力。

(2) 重视实用性和可操作性。本书偏重于实际操作方法的讲述，目的是为那些从事网络管理及网络安全规划与设计的从业人员提供一定的安全操作参考。另外，对网络安全感兴趣的读者也可以从本书中学习到网络防御的基本知识和技巧。

(3) 以“应用实例导航”为牵引。本书在介绍各种网络入侵手段与应对措施时，都通过一个应用实例导航进行导入，这些应用实例大多数是作者在实际工作中遇到的问题，旨在为读者解决大型网络安全问题提供思路和借鉴。

(4) 网络安全产品选择具有代表性。目前，网络安全产品众多，使用与配置方法各不相同，但原理基本相同。由于 Cisco 和 Microsoft 所生产的网络安全产品在局域网使用广泛，技术先进，本书就以 Cisco 和 Microsoft 的网络安全产品为例，介绍如何实施和管理网络安全。

4. 本书读者

本书既可作为大中专院校的教材，也可作为各类培训班的培训教程。此外，本书也可作为企业网络管理员及网络爱好者、企业 IT 经理以及网络安全工程师的参考用书。

本书由胡文启、徐军、张伍荣编写，全书框架结构由何光明拟定。另外，许勇、吴婷、陈玉旺、许娟、吴蕾、姜萍萍、赵传申、杨明、杨萍、陈芳、范荣钢、钱阳勇、陈智、张凌云、王国全、丁善祥等同志对本书出版亦作出了重要贡献，在此一并感谢。

限于作者水平，书中难免存在不当之处，恳请广大读者批评指正。

编　者

目　　录

第 1 章　网络安全基础

随着 Internet 的迅猛发展以及电子交易的逐渐增多，基于网络的应用程序和服务使所有公司信息资源的安全风险增加。在资产评估方面，信息资产将成为一种非常重要的受保护资产。如果没有充分的保护，个人、企业和政府将面临巨大的资产流失风险。

网络安全主要是保护数字资产的机密性和完整性，以及确保这些数字资产的可用性。根据这个原则，本章将介绍如何应对多种网络威胁。通常，这些威胁源于不同种类的攻击行为，或者来自一些软硬件的错误配置以及最终用户的疏忽等。有一点是值得我们注意的，我们无法完全消除网络威胁，但我们可以对网络进行有效的安全评估和风险管理，从而使网络威胁降到最低。

通过本章的学习，读者应掌握以下主要内容：

- ✧ 网络安全的基本原理
- ✧ 攻击事件的来源
- ✧ 网络安全的关键要素
- ✧ 如何提高用户安全意识
- ✧ 如何进行网络安全分析

1.1　网络安全的基本原理

1.1.1　网络发展及需求

传统的网络安全观点认为，封闭式的网络具有较高的安全性，而且当时的运营商受技术限制，远程接入的封闭式网络通常仅能使用调制解调器拨号的方式，如图 1-1 所示。

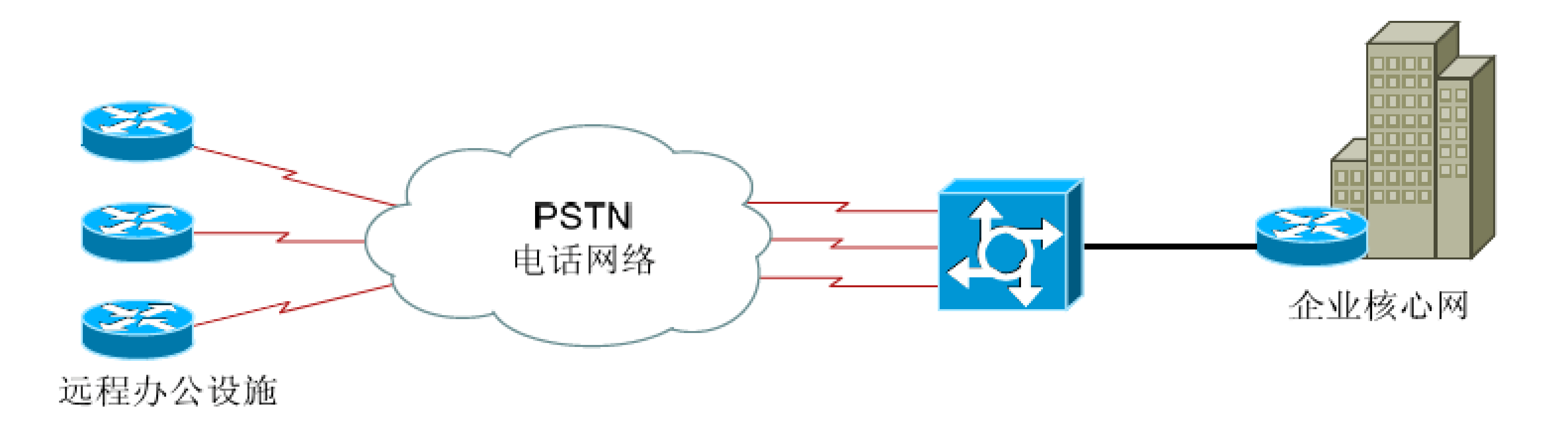


图 1-1　封闭式网络

但随着 Internet 的发展，各种新技术不断涌现，网络交流更加顺畅，企业办公也逐渐转移到 Internet 这样开放式的网络上。这就带来一个矛与盾的问题：一方面需要将自己公司的信息公布于众，另一方面又需要将敏感数据仅供授权用户访问。

大量的安全风险是由局域网和个人电脑接入 Internet 而产生的。特别是对于公司，它的一些公共接口的服务器和电脑成为泄密的最大来源。而这些供访客和公众使用的设备，通常没有专人维护，导致系统和应用软件补丁更新不及时，从而非常容易受到攻击。通常我们把这种攻击叫做“0 day”入侵，因为这些入侵借鉴已有的漏洞报告，仅需要 0 天的时间就能完成攻击。

我们对于这种攻击的解决办法是采用深度的防御模型，也就是说，使用防火墙将公共领域的服务器和接入的计算机与核心工作区域隔离。在防火墙的产品定义中，通常借鉴军事上的定义方式，将与公众接触的计算机定义为非军事化区域(Demilitarized Zone，DMZ)，简称 DMZ 区域。例如 Web 服务器、邮件服务器、DNS 服务器、前台查询计算机等。而内部的文件服务器、数据库服务器等关键应用都放置在军事化区域中，受到良好的保护，如图 1-2 所示。即便 DMZ 区域的设备因某些“0 day”攻击而导致瘫痪，黑客也会因受到防火墙的隔离而无法访问内部网络。

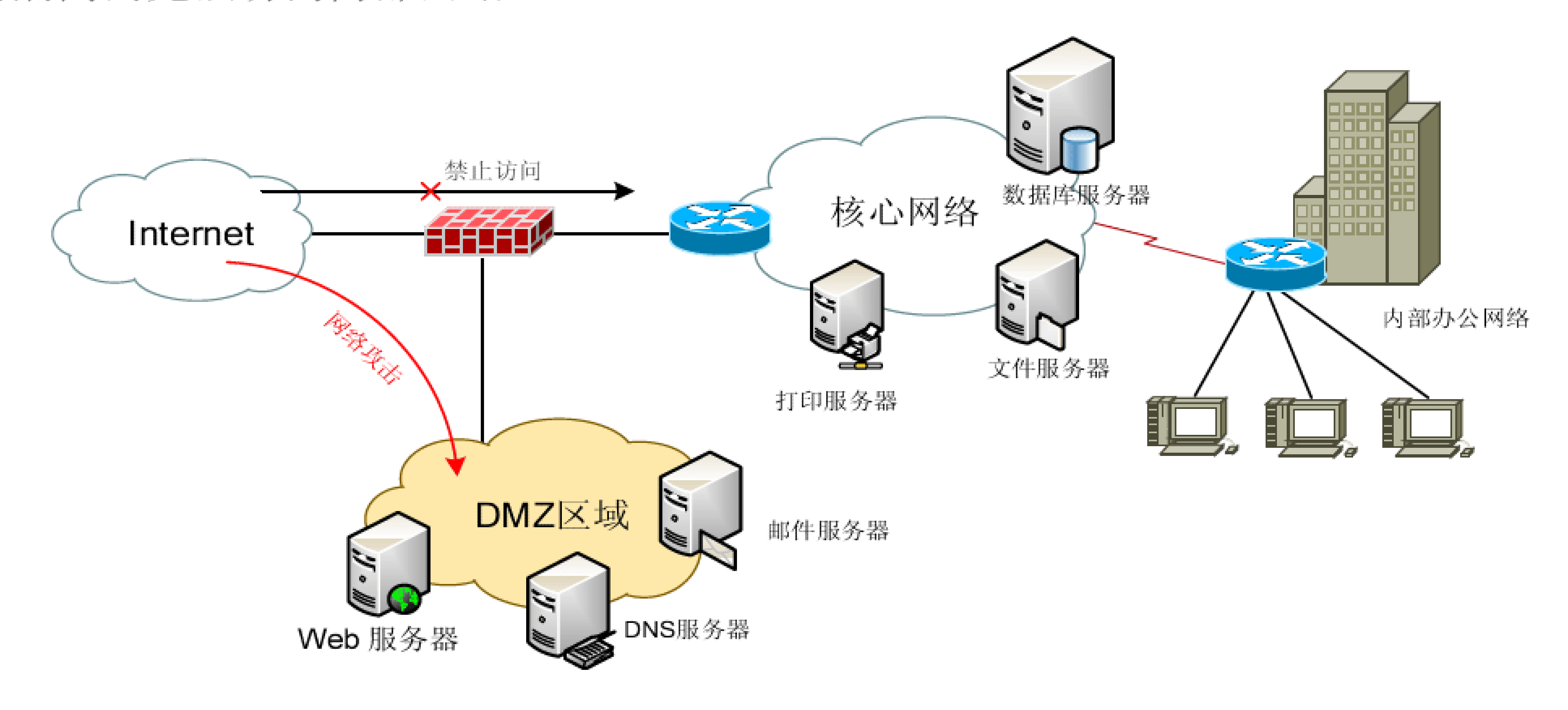


图 1-2　DMZ 区域

在此，虽然我们抵御了来自外部的攻击，但有一个因素我们必须考虑，来自内部的威胁通常更大。最近的统计数据表明，80%的网络安全问题来自网络内部。所以我们需要采取一些措施来降低内部的威胁。首先需要限制内部用户的访问权限，使得只有授权用户能够连接到数据库服务器、文件服务器、打印服务器等关键应用服务器。随着技术的发展，U 盘、移动硬盘也成为非常容易泄密的工具，所以也需要限制内部用户使用外接硬件的权利，避免数据被窃；同时也需要避免非授权电脑接入内部网络。在这个方面，通常使用的是 NAC 接入访问控制系统和 Windows 的一些组策略来完成，稍后的章节我们将详细介绍。

本书使用的一些常用图例，具体如图 1-3 所示。

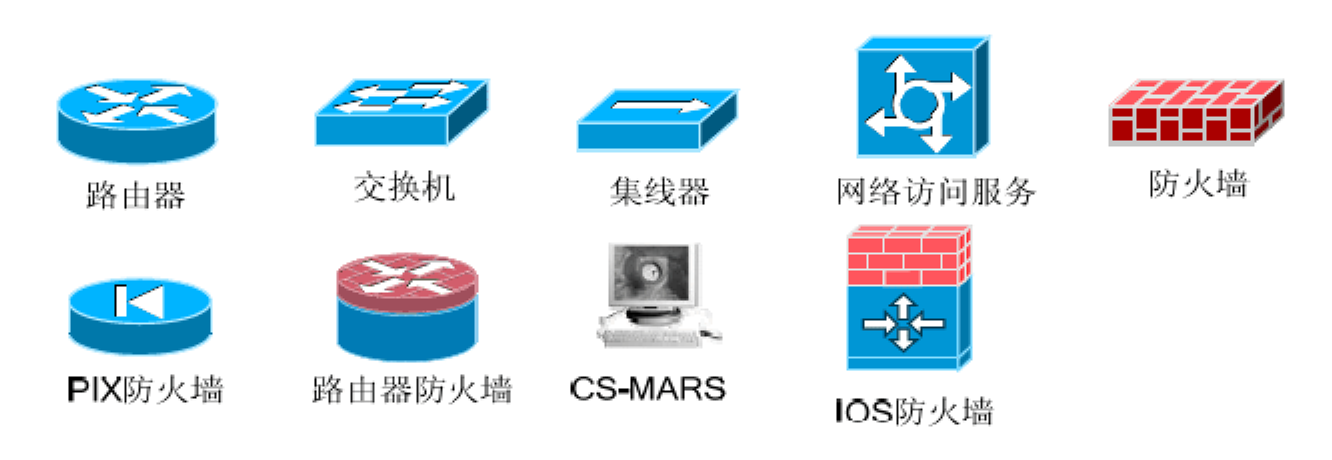


图 1-3　图例

1.1.2　攻击事件的来源

除了少部分黑客基于研究目的带来的攻击外，大多数的网络攻击出于一些特定的目的。根据《2006 年度中国网络安全报告》的结论，截止到 2006 年 12 月 25 日，据不完全统计，中国网络发生的网络攻击事件中，脚本入侵比例为 53%，拒绝服务攻击比例为 26%，漏洞利用比例为 13%，暴力猜解比例为 8%，社会工程学比例为 5%，其他方法为 1%。但与 2005 年同期相比，2006 年度的网络攻击事件要多出 1 倍之多。据不完全统计，自 2006 年 1 月 1 日起，截至 2006 年 12 月 25 日，中国网站被篡改的数量达 25 820 个。其中政府类网站有 3661 个；企业类网站为 11 828 个(其中博客运营类被攻击数量达 1683 个)；教育\培训类被攻击网站数量达 2216 个，其中：中、职专及中小学网站占 73.5%(1628 个)，大学网站的二级网站占 18.0%(398 个)，培训类机构为 127 个，大学一级域名站点为 63 个。

下面是 2006 年出现在我国几个著名的攻击的事件。

- 2006 年 5 月 27 日，某市的区政府服务器被入侵并植入香港汇丰银行的假冒网站。2006 年 4 月，国外多家媒体以《中国的银行网站被利用作 Phishing》为题，报道了中国某银行网站被植入假冒 Paypal 网站的事件。
- 2006 年 6 月 19 日，D 市某区政府网站邮件服务器被入侵并植入电子港湾(eBay)的假冒网站。
- 2006 年 9 月 12 日，著名搜索引擎百度遭受有史以来最大规模的不明身份黑客攻击，导致百度搜索服务在全国各地出现了近 30 分钟的故障。
- 2006 年 9 月 21 日，某域名服务商“新网”域名解析服务器发生故障，造成超过 30%在其上注册的网站无法访问长达 20 小时。“新网”官方确认此次断网事件是黑客所为。此事件被称为中国互联网的“9 • 21 事件”。

在具体的攻击手法上也有变化，猜测口令、物理入侵、安装键盘记录设备以及盗窃笔记本电脑等传统方式的攻击成功率逐渐下降，而 SQL 注入、钓鱼、拒绝服务攻击以及各类木马病毒等攻击频率急剧上升。更值得关注的是，内部人员滥用网络、盗窃关键数据的事件也在上升。随着无线网络的使用，无线网络入侵也成为一个非常值得关注的焦点。

1.1.3　网络安全的关键要素

虽然 Internet 的成功带来了全球信息化的一次巨大飞跃，但是它必须以保护有价值数据和网络资源免受篡改和入侵为基石。

1. 网络安全目标

M. Fites、P. Kratz 等在《Control and Security of Computer Information Systems》中提出了一个被广泛采用的网络安全性设计建议。该建议包括以下内容。

- 确定要保护什么。
- 确定尽力保护它免于什么威胁。
- 确定威胁的可能性。
- 以一种相对廉价的方法来实现资产保护的目的。

✧ 不断地检查这些步骤，发现弱点就进行改进。

2. 资产评估

资产评估用于实现网络安全目标的第一步，需要确定保护什么。通常的资产评估仅对网络设备(例如交换机、路由器、防火墙、电脑)等实物以及关键数据进行评估，而忽视了这些设备上的配置信息、用户访问权利，随着 DDoS 攻击的增加，可用带宽和访问速率也成为资产评估一个不可缺少的部分。当然资产评估随着需要保护的资产数量增长还会出现变化，下面列举了一些重要的网络资产。

✧ 网络设备：路由器、交换机、防火墙、入侵检测设备。
✧ 网络数据：数据服务器、邮件服务器、Web 服务器等。
✧ 网络带宽：链接网络的链路带宽和速度，以及冗余备份线路。
✧ 个人电脑：个人电脑是否携带关键数据以及个人电脑安全防护。
✧ 任意时刻通过网络的消息是否安全。
✧ 网络身份识别是否有效。

3. 威胁评估

根据网络安全目标，完成资产评估后需要对威胁进行评估。通常的攻击手段主要有 3 种类型。

✧ 未授权的网络资源访问。
✧ 未授权的网络数据修改和操作。
✧ 拒绝服务。

授权是网络威胁的一个重要环节，给用户授权通常可以使用很多方式，最常见的身份认证协议是 RADIUS (Remote Access Dial-In User Service，远程访问拨入用户服务)、TACACS+ (Terminal Access Controller Access Control System，终端访问控制器访问控制系统 Plus)、Kerberos 等。当然，还有新兴的数字证书、智能卡、生物界定和目录服务等。

4. 网络安全策略

当完成对威胁的评估后，就需要进行相应安全策略的指定工作了。按照 RFC-2196 站点安全手册的建议，可以从如下几个方面入手指定相应的安全策略。

1) 提供服务和保证安全

每个提供给用户的服务都会带来安全上的风险。对于有的风险高于受益的服务，管理员可能宁愿选择取消它而不去再试图保护。

2) 易用性和安全性

使用起来最简单的系统是允许任意用户不使用密码就可以访问的系统，也就意味着没有任何安全性。要求密码使得系统有些不方便，但是却更安全了。需要设备产生的一次性密码使得系统更不方便了，但是要安全得多。

3) 保障安全的开销和发生损失的风险

保障安全的开销有许多种：金钱(购买像防火墙和一次性密码生产器这样的安全设备和软件的花销)、性能(加密和解密要花费时间)和易用性。发生损失的风险也有许多级别：泄密(信息被未授权的个人所阅读)、数据丢失(信息错误或消除)和服务损失(填充数据存储空间、占用运算资源和拒绝网络服务)。每种开销都要和每种损失作权衡。



RFC-2196 中规定了一个好的网络安全策略应包括如下几个方面。

- ✧ 计算机技术购买的指导方针。它指出什么是必需的或首选的，指出安全的特征，这些对于已存在的购买的政策和指导方针将是补充。
- ✧ 隐秘政策。它规定了对隐秘的合理期望，比如怎么对待电子邮件的监视、按键记录和用户文件访问。
- ✧ 访问政策。它通过列举用户、操作人员、管理者允许使用的功能，规定了存取访问的权利和特权，从而保护资产不损失或泄密。它会在外部的连接、数据交流、网络连接装置和给系统添加新的软件等情况下，提供指导方针。它同时也要列出需要声明的信息(例如，连接信息应该提供关于授权使用和线上监视的警告，而不是仅仅简单地显示“欢迎”)。
- ✧ 责任政策。它规定了用户、操作人员、管理者的责任。它应该明确谁有审查的能力，并提供突发事件的处理方针(就是如果发现可能被入侵了要做什么和联系谁)。
- ✧ 认证政策。它通过有效的密码政策建立信任，使用对远程身份认证设置指导方针的方法或使用认证设备(这里指一次性密码和产生一次性密码的设备)。
- ✧ 可用说明。它预计了用户可以使用的资源。它应该考虑到冗余和恢复的情况、特殊的工作时间和停机维护的时期。它应该也包括系统和网络失败报告的连接信息。
- ✧ 信息技术系统和网络维护政策。它描述了人们被允许怎样运用技术手段进行内部和外部的维护。这里要考虑的一个重要话题是是否允许远程维护，这种访问怎么控制。这里要考虑的另一个问题是外购和怎么管理它。
- ✧ 侵害报告政策。它指出哪种侵害(秘密还是安全，内部还是外部)必须报告，报告给谁。无危险的气氛和匿名报告将会导致被发现的侵害都更可能报告上来。
- ✧ 支持信息。它向用户、职员和经理提供每种侵害的联系信息；怎么处理外部的关于安全事件的询问或什么可以当做秘密私有的指导方针；安全程序和相关信息的交叉参照，例如公司政策和政府的法律规章。

对有些安全政策(如在线监控)可能需要一些调整，安全政策的创建者在产生政策的时候应该考虑寻求法律援助，至少这些政策必须让法律顾问过目一下。一旦安全政策已经建立，应该清楚地与用户、职员和经理进行交流，让所有人都写下一句话表明他们已经阅读过，并且同意遵守这个政策。最后，安全政策应该被当做一个正式的基本政策进行重新检查，看看它是否成功地支持了安全需求。

1.1.4　用户安全意识

正如前述，现在较多的安全漏洞都是由用户不经意间的一些操作引起的，每个公司有必要为员工提供足够的训练来教育他们如何安全地使用这些设备。这种训练需要所有设计、实现和维护网络的人员参与。同时除了技术类的培训外，还应该加强内部控制等。负责网络安全的人员应该对安全技术、威胁评估、标准威胁处理流程及系统补丁及时升级等进行进一步的练习。而作为账号管理员，或者密码分发人员，需要在职员提供完全真实的信息后才能进行相关口令的处理，但很多时候口令的泄露是因为没有被要求出示足够详细的证件。

在终端安全方面通常可以采用安全代理工具来完成一些安全性检查，同时，还可以通过 NAC 网络接入控制来限制未授权的电脑接入网络。

1.2 网络安全实例分析

应用实例导航：A 大学网络安全风险评估

※场景呈现

A 大学是一所历史悠久的全国重点高校，校园网络相当复杂，同时它又是某国家网络的骨干结点，所以网络安全是一个非常重要的环节。众多的服务器和接入计算机使得网络维护难度相当大，因此需要对整个网络进行相应的安全评估和风险分析，然后做出适当的安全升级方案。

※技术要领

(1) 资产评估；
(2) 风险分析；
(3) 制定安全策略。

1.2.1 资产评估

首先要做的仍旧是资产评估，通过资产评估来确定网络需要保护什么。A 大学的资产如下所示。

- ✧ 接入用户。学生宿舍网络用户约 4 万人，办公区各院系共有近 3000 台计算机接入网络。
- ✧ DNS 服务器、邮件服务器、教学视频等点播服务器、BBS 服务器、数据库服务器、存储服务器、学生选课系统服务器及财务和在线办公室服务器等。
- ✧ 链接各校区骨干网链路为 10Gbps 以太网。
- ✧ 链接 ISP 为教育网 3Gbps，中国电信 2Gbps，中国网通链路 1Gbps，中国移动链路 1Gbps。
- ✧ 教育网某骨干结点，其中运营商级路由器 10 台。
- ✧ 交换机、路由器等设备来自 Cisco、Extreme、Foundry、实达、华为等多个厂商。
- ✧ 用户接入采用 IP-MAC 绑定策略。
- ✧ 简单的流量监控系统。
- ✧ 网络管理员较少，并且各信息系统开发独立。
- ✧ 仅有简单的网络安全监控设备。

以上是 A 大学所有与网络有关的硬件资产分析，这些网络设备是要保护的资产，当然资产中最重要的并不是这些硬件资产，而是各个数据库中的数据。从后面的实例我们将逐渐看到数据的价值远远高于这些硬件产品。

1.2.2　风险分析

就校园网络而言，A 大学的网络规模是相当庞大的，相当于一个中小型城市的规模了。而在网络安全方面，基本上没有投入。2006 年的《黑客防线》上也介绍了在类似情况下较多的网站被成功入侵的案例。我们需要对整个网络进行风险分析，并排定系统重要程度，以采取不同策略进行保护。下面对每项资产进行分类。

- ✧ 保密性：避免未经授权数据被传送到第三方。
- ✧ 完整性：确保数据不被修改和破坏。
- ✧ 可用性：网络是否联通，应用程序是否可用，服务不正常时对网络的影响程度。

表 1-1 所示为按照以上分类制作的风险评级表，根据各类的重要程度分别定为 1～10 分。

表 1-1　A 大学部分网络资产风险评级表

资　产	保密性	完整性	可用性
教务系统	5	5	3
财务系统	3	5	4
核心网络设备	4	2	5
Internet 链路	2	2	4
学生宿舍网络	2	2	2
邮件服务器	3	5	5

风险分析结论就是各项的总分，根据不同的特点可以采用不同的安全措施，并且根据安全等级的不同，采用不同的设备进行安全控制。例如关键服务器需要灾难备份的功能，而学生宿舍网络的安全需求则相对低很多。

1.2.3　制定安全策略

完成风险分析后，就可以开始有针对性地制定一系列风险策略了。

1. 关键服务器及网络设备

对于财务、教务系统的服务器以及 Mail、DNS、存储等关键服务器采用集中托管的方式，并加载入侵检测和防火墙系统，同时做好对数据完整性要求很高的系统备份工作。在使用时间方面，对于某些系统进行限时，限制 IP 地址访问。

对于关键网络设备，例如核心路由器、汇聚路由器等，需要进行双链路备份。A 大学在最近一次网络升级中，将传统的分层网络结构进行了扁平化处理，保证了结点备份，同时也保证了关键设备的冷备份，即便出现重大故障也能快速恢复。

2. 访问策略

对于 A 大学网络而言，需要一个相对安全的访问策略。例如，VPN 接入仅部分教师和工作人员能够访问链接，并且关键服务器采用拨入后的二次认证，以防受到攻击。对于新

的员工需要访问某些资源，则必须由该部门主管和安全部门的主管一起确认后才能开通。这样可以避免因工作失误导致的密码泄露。

对于无线网络，为了方便用户接入，同时又不失安全性，A 大学采用了多个 SSID 接入的方式，相对简单的 Web 身份认证接入采用可以广播的 SSID，并且不采用加密策略。而对于可以自由访问校内资源的网络则采用了 802.1x 和 WEP 认证的接入方式，并且 SSID 不广播。这样就很好地在安全性和易用性方面取得了平衡。

3. 身份认证

为了识别用户身份，A 大学采用了基于 Radius 的统一身份认证。邮件系统、个人存储、无线网络身份认证、各种信息查询等均使用统一的账号。

同时对于所有的网络设备，仅网络中心人员有访问 Radius 账号的权限。对于 Radius 服务器的权限应该仅掌握在安全主管的手中。

4. 办公网络安全

A 大学曾经因为某办公室老师私开 FTP 服务器时设置了弱密码而导致一些敏感数据泄漏，所以，对办公区的老师需要进行相应的安全培训。同样学生将电脑接入网络的时候，也需要注意自己的电脑是否会对网络造成影响。A 大学发布了《A 大学网络接入最低安全需求》，并要求所有用户按照该要求执行。

5. 安全事故处理

当出现安全事故后，或者发生数据盗用行为后，需要建立一套手工和自动报告的系统。一方面可以通过 Cisco Works、Solarwinds 等网管软件汇报；另一方面，也可以通过一些员工或者其他人匿名汇报隐藏的攻击危险。

对于所有的日志，安全主管必须及时响应和处理，并对故障进行快速修复。

1.3 网络的漏洞与攻击

1.3.1 常见网络弱点

1. TCP/IP

TCP/IP 是一种开放式的标准，在 Internet 上被广泛使用，但是存在很多安全漏洞。例如 HTTP、FTP 和 ICMP，其本质上就是不安全的；ICMP 对于消息不作验证就可以发出，当收到后，可以继续重定向发送到下一个设备上；而对于 SNMP 而言，它是网络管理中用得最多的消息，但是版本 1 和版本 2 中的身份验证和访问控制等功能相当的薄弱，而且不具有保密性；对于 TCP/IP 而言，容易受到 SYN flood 攻击，也是该协议不完善的一个地方。

所以需要一系列相对安全的处理方式来对这些漏洞进行弥补。通常对于远程结点的访问采用基于安全的 IP 协议 IP Sec 来实现。而对于其他关键数据在发送的时候已经做好了相应的处理。

2. 系统安全漏洞

对于操作系统而言，也存在很多安全漏洞，许多 Web 服务器及其他关键数据受到的攻击都来自这些漏洞，通常 Windows XP/2003/Vista 以及 Linux、UNIX、MacOSX 都存在安全漏洞，特别应值得注意的是，这些安全漏洞通常在发布后几个小时，就有主机因这些漏洞而被攻破。

3. 网络设备漏洞

很多网络设备也有漏洞，例如 Cisco 的路由器和交换机所使用的 IOS 软件通常也会爆出一些安全性的漏洞，另外像 Juniper 使用 FreeBSD 系统作为控制平台，所以也会出现一些安全性漏洞。这些漏洞将会给网络带来致命性的打击。

1.3.2 常见攻击方法

网络攻击，从 20 世纪 80 年代单纯使用密码猜测的方式，发展到现在的 SQL 注入、网络钓鱼、跨站攻击、溢出漏洞、拒绝服务攻击及社会工程学等技术的使用，攻击难度越来越低。网络变得十分脆弱，一方面因为威胁变得越来越复杂，另一方面因为实施这些威胁所需要的知识越来越简单。

1. SQL 注入

随着 Internet 的发展，基于 DBMS 的 Web 查询数据库逐渐增多，但是 Web 制作行业门槛不高，程序员的水平和经验也参差不齐，相当大一部分程序员在编写代码的时候没有对用户输入数据的合法性进行判断，致使程序出现安全隐患。攻击者可以通过互联网，构造一个精妙的 SQL 语句注入到 DBMS 中，从而获得访问权限。

SQL 注入手法相当灵活，能够根据不同的情况进行具体的构造。通常，几乎所有的防火墙对通过万维网访问的数据库请求无法发出及时的警报，所以 SQL 注入具有极高的隐藏性。下面来看一个常见的 SQL 注入的例子。

通常访问一个网站时，会看到如下格式的 URL 信息：

```
http://www.jam.cn/show.asp?ID=521
```

它表示服务器正在运行类似于“Select * from 表名 where 字段="&ID"”的查询，并且将查询结果返回客户端。此时可以采用如下的方式注入：

```
http://www.jam.cn /show.asp?ID=444 and user>0
```

这时，服务器运行“Select * from 表名 where 字段=444 and user>0”这样的查询。当然，这个语句是运行不下去的，肯定出错。例如，错误信息如下：

```
• 错误类型：
Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)
[Microsoft][ODBC SQL Server Driver][SQL Server]将 nvarchar 值 'jam' 转换为数据类型为 int 的列时发生语法错误。
show.asp， 第 37 行
```

从这个出错信息中，可以获得以下信息：该站使用的数据库是 Microsoft SQL Server，连接方式采用 ODBC，连接账号为 jam。

我们猜测网站管理员账号在表 login 中，管理员账号为 admin，若想知道管理员密码，可以从客户端接着提交这样一个网址：

```
http://www.jam.cn /show.asp?ID=444 and (Select password from login where
user_name='admin')>0
```

返回的出错信息如下：

```
• 错误类型:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)
[Microsoft][ODBC SQL Server Driver][SQL Server]将 varchar 值 'ciscojam' 转
换为数据类型为 int 的列时发生语法错误。
/show.asp， 第 37 行
```

在错误信息中，ciscojam 就是管理员的密码。

2. 网络钓鱼

网络钓鱼，英文为“Phishing”(因为它首先被黑客使用在电话线路上，所以用 Phone 的前两个字母代替了 F)。钓鱼攻击通常采用大量发送垃圾电子邮件的形式，诱骗收到邮件的用户发送自己相关的金融账号和密码，以及身份证号等其他号码，继而盗取现金。

蒙骗方法通常很简单，例如注册 www.lcbc.com 来模仿www.icbc.com等，粗心的用户会忽视这样的拼写错误。在中国工商银行的 hotspot.jsp 页面上，也可以通过对 column 函数进行修改直接伪造页面。代码如下：

```
http://www.icbc.com/news/hotspot.jps?column=Hacked%20by %20jam
```

结果如图 1-4 所示。



图 1-4　伪造页面

3. 分布式拒绝服务

DDoS(Distributed Denial of Service，分布式拒绝服务)攻击很简单，即用大量的主机来访问网络中的某一台机器，导致其性能下降影响正常的服务。DDoS 是一种简单的攻击工具，当某些 IDC 机房服务器被攻破后，将其作为 DDoS 攻击源，后果将不堪设想。同时，对于

DDoS 攻击，如何找出源地址，也是一个非常困难的事情。

由于 DDoS 非常容易实施，并且成功几率非常高，所以在安全事件中，这类攻击增长非常迅猛。在我国的部分 ISP 统计数据中显示，有些攻击就来自 IDC 机房，例如不同的网络游戏服务商之间的竞争等。而且在过去几年较为重大的几起安全事件中，几乎都是由 DDoS 攻击引起的。

4. Rootkit

由于网络安全产品正在变得越来越强大，攻击者不得不增加赌注。2006 年，Rootkit 技术开始被广泛地应用，而且有不断增长的趋势。Rootkit 其实是一种功能更强大的软件工具集，能够让网络管理员访问一台计算机或者一个网络。一旦安装了 Rootkit，攻击者就可以把自己隐藏起来，在用户计算机中安装间谍软件和其他监视敲击键盘以及修改记录文件的软件。虽然微软发布的 Vista 操作系统能够减少某些 Rootkit 的应用，但是 Rootkit 还是 2007 年黑客普遍使用的技术。据赛门铁克称，用户模式 Rootkit 策略目前已经非常普遍，内核模式 Rootkit 的使用也在增长。

5. 跨站脚本

通常对于动态输入有 URL 参数、表格元素、cookies 等几种形式。下面为一个网站使用 cookies 来获取用户名的代码。

```
<%@ Language=VBScript %>
<% If Request.Cookies("userName") <> "" Then
Dim strRedirectUrl
strRedirectUrl = "page2.asp?userName="
strRedirectUrl = strRedirectUrl & Response.Cookies("userName")
Response.Redirect(strRedirectUrl)
Else %>
<HTML>
<HEAD>
<TITLE>jam.cn </TITLE>
</HEAD>
<BODY>
<H2>jam.cn</H2>
<FORM method="post" action="page2.asp">
Enter your jam.cn username:
<INPUT type="text" name="username">
<INPUT type="submit" name="submit" value="submit">
</FORM>
</BODY>
</HTML>
<% End If %>
```

假设，第二页用于返回用户名以示欢迎。

```
<%@ Language=VBScript %>
<% Dim strUserName
If Request.QueryString("userName")<> "" Then
strUserName = Request.QueryString("userName")
Else
Response.Cookies("userName") = Request.Form("userName")
strUserName = Request.Form("userName")
End If %>
<HTML>
```

```
<HEAD></HEAD>
<BODY>
<H3 align="center">Hello<%= strUserName %> </H3>
</BODY>
</HTML>
```

当用户正常输入文字时，一切都很正常。如果输入 Script 代码：

```
<script> alert('hacked by jam .';</script>
```

JavaScript 警告对话框就会弹出来：在下一次访问时，这个警示对话框同样会出现。这是因为这个 Script 代码在第一次访问的时候就已经留在 cookies 中了。

1.3.3　攻击分类

在进行安全策略指定的时候，除了对自身服务器进行威胁评估外，还应该对各种攻击类型进行安全评估，并对威胁较大的攻击类型进行特别的处理。Cisco 安全架构师 Sean Convery 在《Network Security Architectures》中提到了如下分类方式。

- ✧ 读取攻击：在未授权的情况下查看信息。
- ✧ 操作攻击：修改信息。
- ✧ 欺骗攻击：提供虚假信息或虚假服务。
- ✧ 泛洪攻击：使计算机资源发生溢出。
- ✧ 重定向攻击：更改后续信息。
- ✧ 混合型攻击：如上多种攻击的结合。

1. 读取攻击

通常读取攻击主要来自侦查和扫描，并将结果用于后续的拒绝服务攻击。首先对于一个黑客而言，他需要寻找其猎物拥有的是哪些地址段，并且在这些地址段中，哪些是 Web 服务器，哪些是数据库服务器，哪些是 DNS 服务器等。

通常收集到这些数据是相当容易的。通过 whois 可以查询到相应的地址空间，如图 1-5 所示。同时，还可以通过 nslookup 来查询一些特定的服务器，如图 1-6 所示。

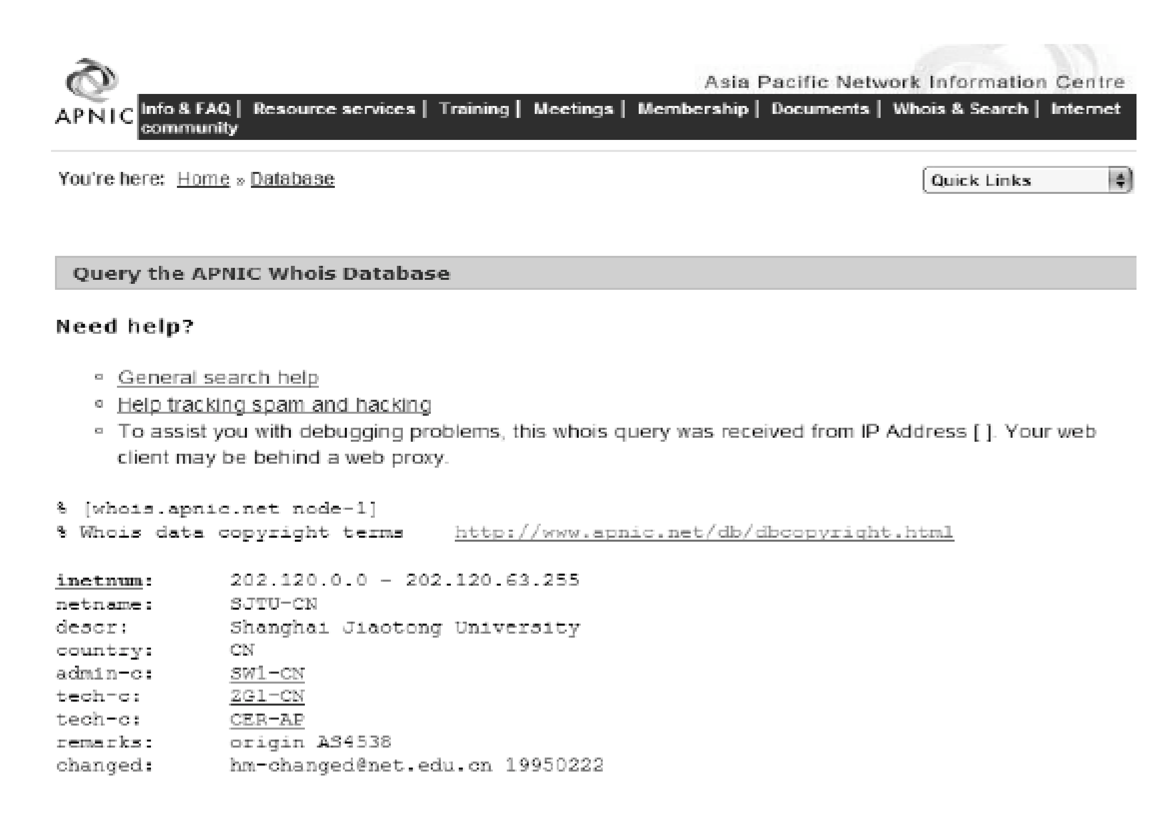


图 1-5　通过 whois 查询地址段

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\>nslookup
Default Server:  dns.sjtu.edu.cn
Address:  202.120.2.101

> bbs.sjtu.edu.cn
Server:  dns.sjtu.edu.cn
Address:  202.120.2.101

Name:    bbs.sjtu.edu.cn
Address:  202.120.58.161

> www.sjtu.edu.cn
Server:  dns.sjtu.edu.cn
Address:  202.120.2.101

Name:    www.sjtu.edu.cn
Address:  202.120.2.102
```

图 1-6　通过 nslookup 查询服务器

当然，有些时候通过访问 Google 或者其他方式能够获取更加详尽的地址段，如图 1-7 所示。

标　题：上海交通大学校内IP地址范围(参考)
发信站：饮水思源 (2002年07月05日21:19:23 星期五)，站内信件

包括主要的服务器，学生地址段

	Network			Netmask	CIDR
1.	202.120.0	~ 202.120.63	64个C	255.255.192.0	/18
2.	59.78.0	~ 59.78.63	64个C	255.255.192.0	/18
3.	211.80.32	~ 211.80.63	32个C	255.255.224.0	/19
4.	211.80.80	~ 211.80.95	16个C	255.255.240.0	/20
5.	202.120.128	~ 202.120.143	16个C	255.255.240.0	/20
6.	219.228.96	~ 219.228.127	32个C	255.255.224.0	/19
7.	218.193.176	~ 218.193.191	16个C	255.255.240.0	/20
8.	202.121.176	~ 202.121.183	8个C	255.255.248.0	/21
9.	202.112.26.0		1个C	255.255.255.0	/24
10.	58.196.128.0	~ 58.196.191	64个C	255.255.192.0	/18
11.	61.164.36.0		1个C	255.255.255.0	/24

合计--------------------------250+64个C

图 1-7　通过校内 BBS 获取所有地址段

在确认这些信息后，对关键服务器进行扫描，并确定某些地址段中有多少主机用于服务。扫描一般采用 nmap (www.inseure.org/nmap)。

首选通过 nmap 来扫描某个地址段中活跃的主机情况：

```
 [root@sjtucs ~]# nmap -sP 10.78.7.0/24
Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2007-05-03 11:37 CST
Host 10.78.7.0 seems to be a subnet broadcast address (returned 12 extra pings).
Host 10.78.7.4 appears to be up.
MAC Address: 00:04:61:68:6B:A9 (Epox Computer Co.)
Host 10.78.7.8 appears to be up.
MAC Address: 00:0E:A6:A7:EC:75 (Asustek Computer)
Host 10.78.7.12 appears to be up.
MAC Address: 00:1A:92:CC:8D:21 (Unknown)
Host 10.78.7.13 appears to be up.
MAC Address: 00:50:8D:5D:50:8D (Abit Computer)
Host 10.78.7.23 appears to be up.
MAC Address: 00:0A:EB:C6:5F:65 (Shenzhen Tp-link Technology Co;)
Host 10.78.7.42 appears to be up.
<-------------------省略------------------>
MAC Address: 00:16:B6:C5:6E:2A (Unknown)
Host 10.78.7.150 appears to be up.
Host 10.78.7.188 appears to be up.
MAC Address: 00:90:8F:05:95:50 (Audio Codes)
```

```
Host 10.78.7.189 appears to be up.
MAC Address: 00:90:8F:05:95:4E (Audio Codes)
Host 10.78.7.254 appears to be up.
MAC Address: 00:01:30:18:4E:30 (Extreme Networks)
Host 10.78.7.255 seems to be a subnet broadcast address (returned 13 extra
pings).
Nmap run completed -- 256 IP addresses (35 hosts up) scanned in 4.707 seconds
[root@sjtucs ~]#
```

然后通过 nmap 来扫描已经打开的端口和系统类型。

```
[root@sjtucs ~]# nmap -O 10.78.7.139
Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2007-05-03 11:45 CST
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on 10.78.7.139:
(The 1658 ports scanned but not shown below are in state: filtered)
PORT     STATE SERVICE
1723/tcp open  pptp
3389/tcp open  ms-term-serv
MAC Address: 00:E0:4C:83:A3:7B (Realtek Semiconductor)
Device type: firewall|general purpose
Running (JUST GUESSING) : Symantec Windows NT/2K/XP (90%), IBM AIX 4.X|3.X
(88%)
Aggressive OS guesses: Symantec Enterprise Firewall 7.0 running on Windows
2000 SP2 (90%), IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/* (88%), IBM AIX v4.2
(87%), IBM AIX 4.2-4.3.3 (87%), IBM AIX v3.2.5 - 4 (87%)
No exact OS matches for host (test conditions non-ideal).
Nmap run completed -- 1 IP address (1 host up) scanned in 34.183 seconds
[root@sjtucs ~]#
```

注意，以上这些主机，90%为 Windows 平台，同时还打开了 3389 个远程桌面的端口，为下一步入侵提供了非常重要的信息。

在侦听方面常常使用 Wireshark 网络协议分析仪，图 1-8 所示为 Wireshark 监听界面。

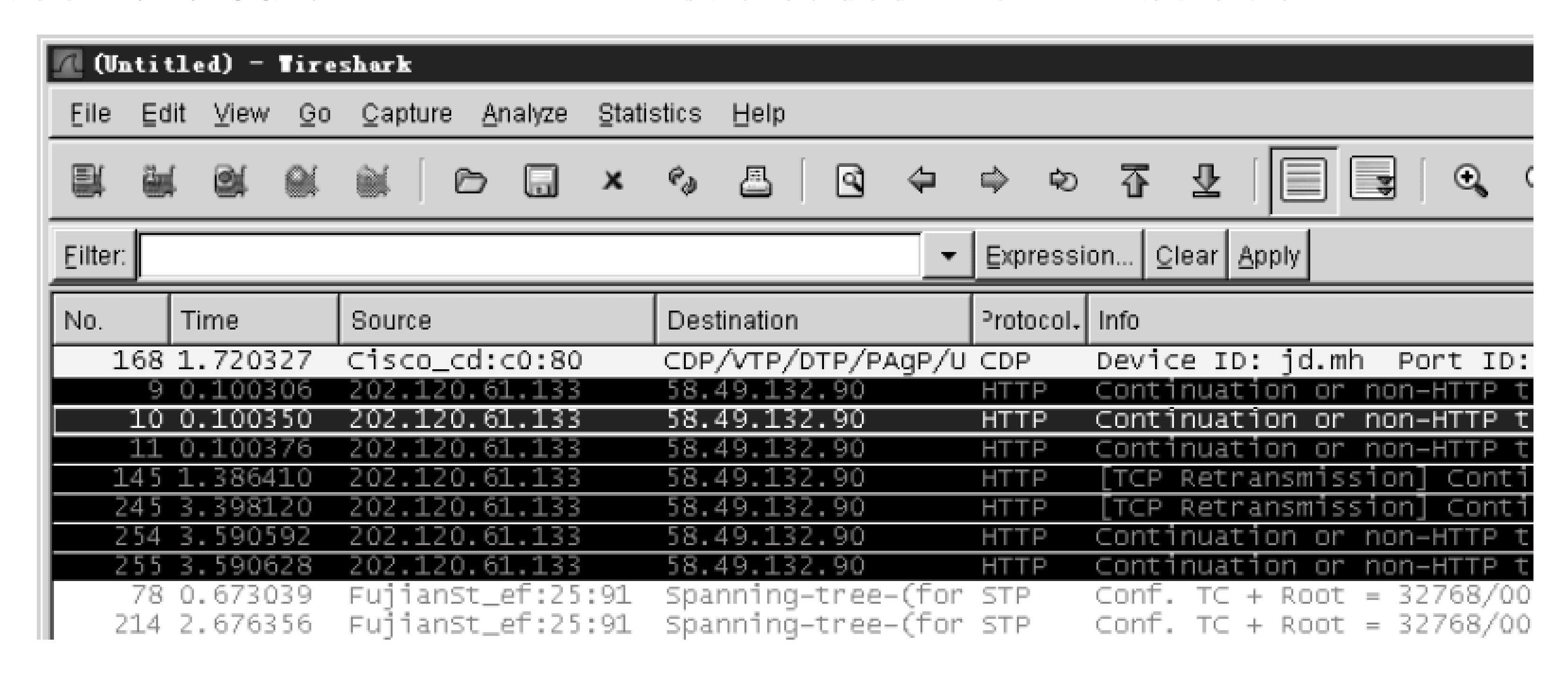


图 1-8 Wireshark 监听

2. 操作攻击

操作攻击以修改数据为目的，前文中的 SQL 注入和跨站脚本便属于这类攻击。当然还有一些早期使用 CGI 的网站，可以直接通过对 URL 进行注入，使得被攻击服务器主动发起到黑客计算机的链接。默认的防火墙规则对外部流入限制严格，但对内部流出不做过多的

限制，因此这种链接一般防火墙无法察觉。

缓冲区溢出也是非常常见的攻击方式。例如某程序员认为，用户合理的输入数据流不会超过 10 个字节，而当恶意攻击者用 1000 个字节的信息进行攻击时，就会导致缓冲区溢出，从而使得其些代码被执行。

3. 欺骗攻击

在欺骗攻击中除了前文介绍的钓鱼攻击外，还有其他很多欺骗方式。现在最常见的方式为 STP 欺骗、VTP 欺骗、ARP 欺骗等。特别是身份欺骗。例如 X.509 证书标准的 IETF 配置文件定义了几个可选的域，这几个域可被包含在一个数字证书中，其中一个为基本约束域，它指明了证书链的最大允许长度，以及此证书是一个证书颁发机构还是一个终端实体证书。然而，Windows 构建和验证证书链的 CryptoAPI 中的 API(包括 CertGetCertificateChain()、CertVerifyCertificateChainPolicy() 和 WinVerityTrust)并没有检查此基本约束域。

拥有一个有效的终端实体证书的攻击者，可以利用这个薄弱环节发布一个从属证书，这个证书尽管是假的，也可以通过验证。由于 CryptoAPI 被用于各种应用程序，将导致许多身份欺骗的攻击行为。在 FAQ 中对这些进行了详细的讨论，包括：建立一个网站，同时假装它是另一个网站，然后通过建立一个 SSL 会话“证实”它自己是一个合法的网站；发送据称属于“其他用户”的数字证书签名的电子邮件；欺骗那些基于证书验证的系统，以便作为一个高级用户得到入口；使用一个据称已颁发给用户可以信任的公司的验证码证书给不良制品进行数字签名。

更加严重的攻击为基于 OSI 模型第二层的 STP、VTP 以及 MAC 地址攻击等，我们将在稍后的章节中专门介绍这类攻击行为。

4. 泛洪攻击

泛洪攻击较多使用在 DDoS 攻击上，目的是让对端服务器无法承受巨大的流量攻击而瘫痪。当然在泛洪攻击上还有其他的攻击手法。

TCP SYN 是泛洪攻击的最早形式，由于 TCP SYN 数据包发出后，不再对响应端送回的 SYN-ACK 进行确认，但是收到 TCP SYN 后服务器将一直保持连接开放状态，在 SYN-ACK 最终被确认的情况下，对持续时间进行确认，服务器还会定期重发 SYN-ACK，在连接拆除之前最多重试 4 次。这样，当发送大量的 TCP SYN 报文到服务器后，服务器将疲于应付而崩溃。

Smurf 攻击原理很简单，它利用一些较小的数据包攻击一些机器，然后使它们产生较大的数据包，通过这样的放大行为，产生大量的流量，使得最终被攻击的主机处于繁忙状态。这样的攻击方式又可以称为增幅攻击。例如一个假冒的广播 Ping 到达回环网络后，该网络的每台主机都向受害者发送不同的 Ping 包，如图 1-9 所示。

当假冒的 Ping 包流量大小为 500Kbps 时，如果局域网内有 200 台主机，则攻击流量将上升为 100Mbps，这样大的流量将很快导致一台服务器处于瘫痪状态。当然，可以通过对交换机进行配置，并通过一些 QoS 的流控策略来避免这样的攻击。

前文已经对 DDoS 攻击做了介绍，DDoS 也是通过前期入侵一系列服务器(特别是寄放在 ISP IDC 的服务器)，一般来说这些服务器拥有较大的带宽，实施 DDoS 攻击相对容易，

并且伴随着一些增幅攻击，对方服务器较容易出现瘫痪。特别是对 DNS 的攻击，会导致域名正常解析出错。

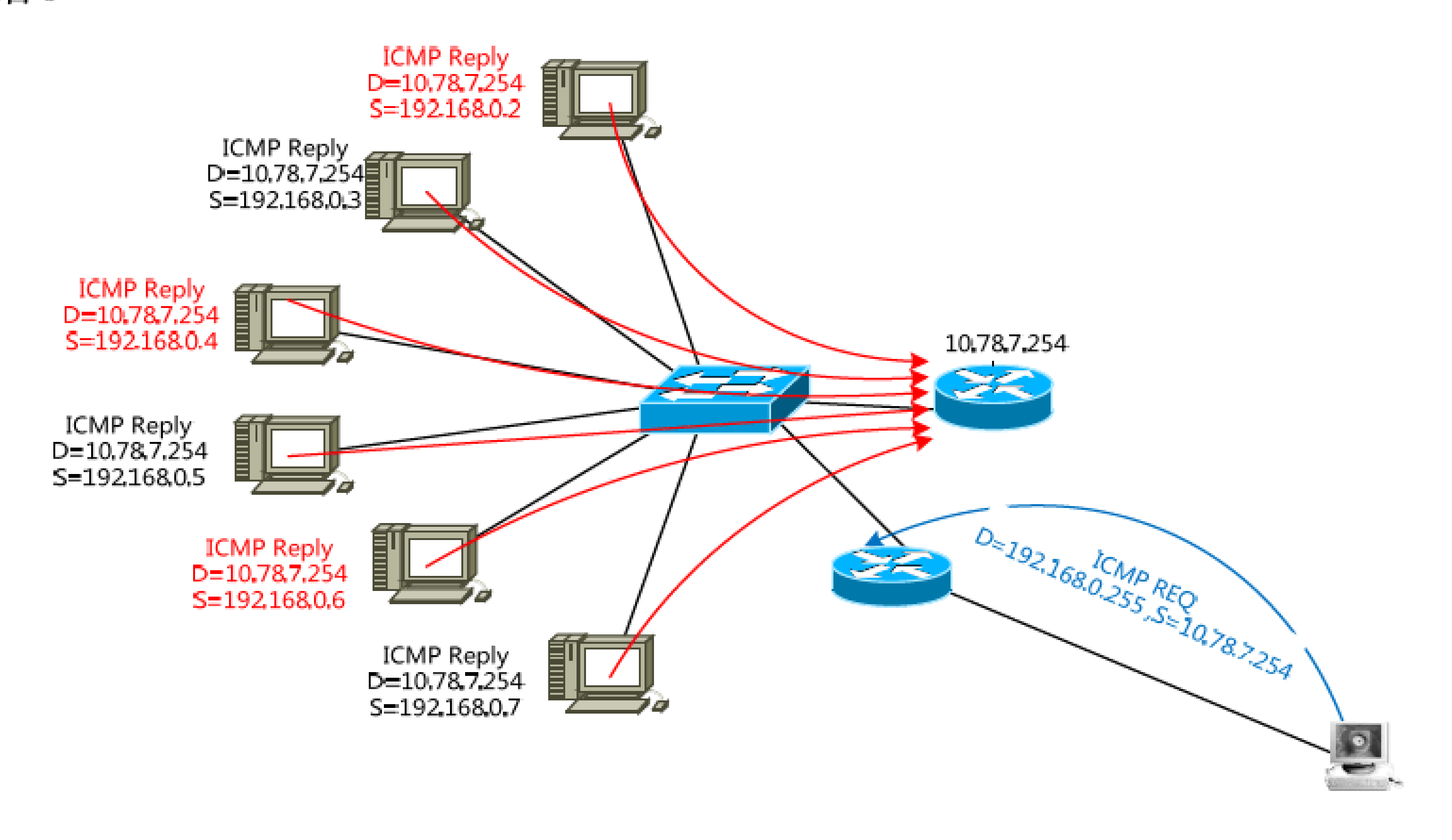


图 1-9　Smurf 攻击

MAC 泛洪攻击则是另一种非常巧妙的形式，每个交换机中都有一个 CAM 表，用于记录端口和相应的 MAC 地址，当这个表满了以后，则采用广播的形式发送。MAC 泛洪就是基于这样一个思路，通过大量的 ARP 报文虚报 MAC，导致交换机 CAM 表溢出，从而通过广播监听到别人的消息。

5. 重定向攻击

重定向攻击也是比较常见的一种攻击行为， ARP 病毒就是这类攻击。ARP 病毒采用虚拟 ARP 报文，让一个网段内所有的主机误认为它就是网关，从而截获所有的报文。由于截获报文后，中毒主机并不转发到真实的网关，这样就导致了整个局域网内同网段主机全部断网。起初它用于“传奇”等网络游戏账号截取上，它通过让其他电脑全部下线，从而在其他电脑试图再次连接服务器时，截获密码。

在重定向中，还有一种为 STP 重定向。利用虚假消息冒充自己的一个接口为 STP 的根桥，从而让交换机进行 STP 重算，则可以将原有的上行接口阻塞，向欺骗接口转发所有的数据。类似的还有，当攻陷一台防火墙后端的机器时，可以采取传输重定向的方法，让这台被攻陷的机器成为访问内网的代理服务器。在重定向类攻击中，还有传统的 IP 重定向及传输重定向等，稍后的章节将对这些攻击做详细的叙述。

6. 混合型攻击

混合型攻击是威胁最大的一种攻击，前文所述的 Rootkit 攻击就属于此类，它们多半为木马病毒类程序带来的攻击。同时蠕虫攻击也渐渐成为一种新的攻击手段。在 Red-Code 爆发 24 小时后，上万台主机受到感染。冲击波等各种新型蠕虫病毒也带来了巨大的威胁。“熊猫烧香”病毒也属于此类。

这类病毒具有非常好的隐蔽性，而较多的杀毒软件无法及时防范这样的病毒，用户稍有疏忽就会对整个网络带来极大的危害。

1.3.4　攻击评估

在对攻击事件进行评估时， Sean Convery 提供了一个很好的评估方案，该方案从四个方面定义了攻击类型的评估。

1. 检测难度

检测难度是指网管员是否能够检测到这些攻击的近似难度。例如有些端口扫描器扫描频率过高将会被很多 IDS 检测到，而 SQL 注入等则相对难以察觉。

2. 攻击难度

攻击难度是指可以在公共场合随意使用的攻击相对来说攻击难度较低采用一些 0 day 漏洞的脚本攻击难度也非常低，而像精妙构造 SQL 语句则成为难度较高的一种攻击方式。

3. 频度

频度是指攻击的频率。端口扫描几乎每天都会发生，而 SQL 注入、ARP 欺骗等发生的频率则相对低得多。

4. 影响

要评估网络安全问题爆发后产生的影响。DDoS 攻击可能对电子商务、政务系统等带来极大的影响和经济损失，而对于国防、军事等重要系统，它的影响则来自数据的丢失和机密的泄露等。

通过对以上四方面按 5 分制打分后，可以通过如下公式计算出总体评价：

$$总体评价=检测难度+攻击难度\times2+频度\times3+影响\times4$$

如果总体评价低于 10，则可以不用过多担心这类威胁；如果总体评价高于 35 则需要关注这类攻击；如果高于 40，则属于高危漏洞，需要及时弥补。Sean Convery 对常见攻击作了如表 1-2 所示的评价。

表 1-2　攻击类型评价表

攻击类型	检测难度	攻击难度	频度	影响	总体评价
缓冲溢出	4	3	5	5	45
身份欺骗	4	3	4	5	42
拨号式扫描	5	4	3	5	42
病毒、蠕虫、木马	3	4	5	4	42
直接访问	2	5	5	3	39
远程控制	4	4	3	4	37
刺探、扫描	4	5	5	2	37
Rootkit	4	2	4	4	36
监听	5	5	3	3	36
应用程序泛洪	3	5	5	2	36

续表

攻击类型	检测难度	攻击难度	频度	影响	总体评价
UDP 欺骗	5	4	3	3	34
无赖设备	3	2	2	5	33
Web 应用	3	3	4	3	33
数据整理	5	4	5	1	32
中间人	4	2	1	5	31
分布式拒绝服务(DDoS)	2	2	3	4	31
TCP 欺骗	5	1	1	5	30
ARP 欺骗和重定向	3	4	1	4	30
TCP SYN 泛洪	3	5	3	2	30
IP 欺骗	3	4	5	1	30
IP 重定向	2	2	2	4	28
Smurf	2	4	2	3	28
传输重定向	4	3	2	3	28
MAC 泛洪	3	5	1	3	28
MAC 欺骗	3	5	1	3	28
STP 重定向	3	3	1	2	20

1.4 本章小结

本章主要介绍了网络安全的一些基本知识，并从宏观上介绍了评估和处理网络安全问题的一些方法，叙述了一些常见的网络安全攻击行为，演示了一些简单的攻击手段和检测手段，介绍了网络安全事件中的攻击行为有哪些，并且使读者能够判断出哪些攻击行为是危险的，哪些行为是可以忽视的。

第 2 章　网络安全解决方案概述

在第 1 章中，我们认识了多种多样的网络攻击行为，并对各种威胁进行了分类和评估。在本章，我们将介绍防范这些威胁的一些方法和解决方案，并对路由器、防火墙、VPN、IPS 等各种网络安全设备的使用有一个初步的了解，然后在后续的章节中逐渐拓展开来详细介绍，并将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，以便有效阻止非法用户进入网络，减少网络的安全风险。

通过本章的学习，读者应掌握以下主要内容：

- 网络安全框架
- 防火墙
- VPN 接入
- 入侵检测
- 常见网络安全解决方案
- DMZ 区域的放置

2.1　网络安全框架

2.1.1　安全基准测试

我们需要采用一个合理的框架来设计一个安全的网络，下面将介绍一些设计安全网络的框架。围绕着在第 1 章中定义的安全策略，我们通过一步步的操作来实现安全网络的目标。通常我们分四步走：一是需要设计一套系统，用于验证用户身份；二是需要设计专门的 VPN 网络用于移动办公和外部访问的数据安全；三是需要建立一套内部补丁快速升级系统，降低“0 day”攻击的威胁；四是组织内部还需要设计严格的管理体制，防范来自内部的入侵。

完成网络安全的建设后，并不是就一劳永逸了。安全产品都有其特有的安全生命周期，所以对于安全产品是否失效，需要经常进行渗入测试。在渗入测试方面，通常使用 Nmap 等工具。这里推荐一个非常出色的安全测试工具 Metasploit Hacker Framework，它现在已经成为网络安全测试的一个基准工具，如图 2-1 所示。

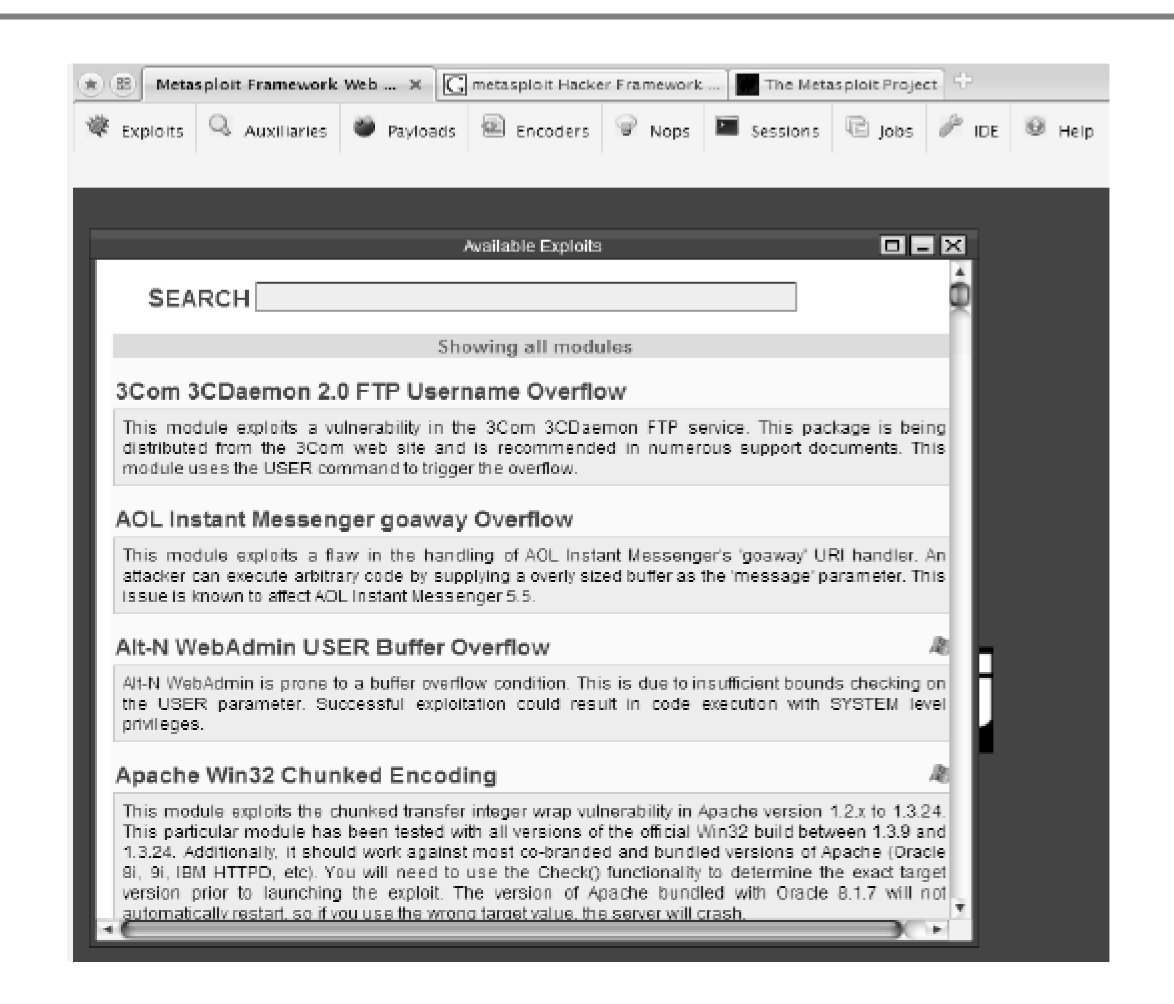


图 2-1 Metasploit 检测工具

2.1.2 安全日志分析

除了安全基准测试外，日常的网络安全监控也是必不可少的，通常实时的监控系统有IDS入侵检测系统、身份认证服务器的日志及其他网络设备的运行日志等。它们所得到的一系列结果对于改善网络安全状况提供了重要的依据。同时随着技术的不断发展，IPS入侵防御系统逐渐登上舞台，对于网络的主动防御提供了重要的帮助。对于不同系统回报的安全日志也进行了很好的整合，Cisco 提供了安全监控、分析和响应系统(Crisco Security Mornitoring，Analysis and Response System，CS-MARS)，它可以有效并且直观地反映攻击事件，如图2-2所示。

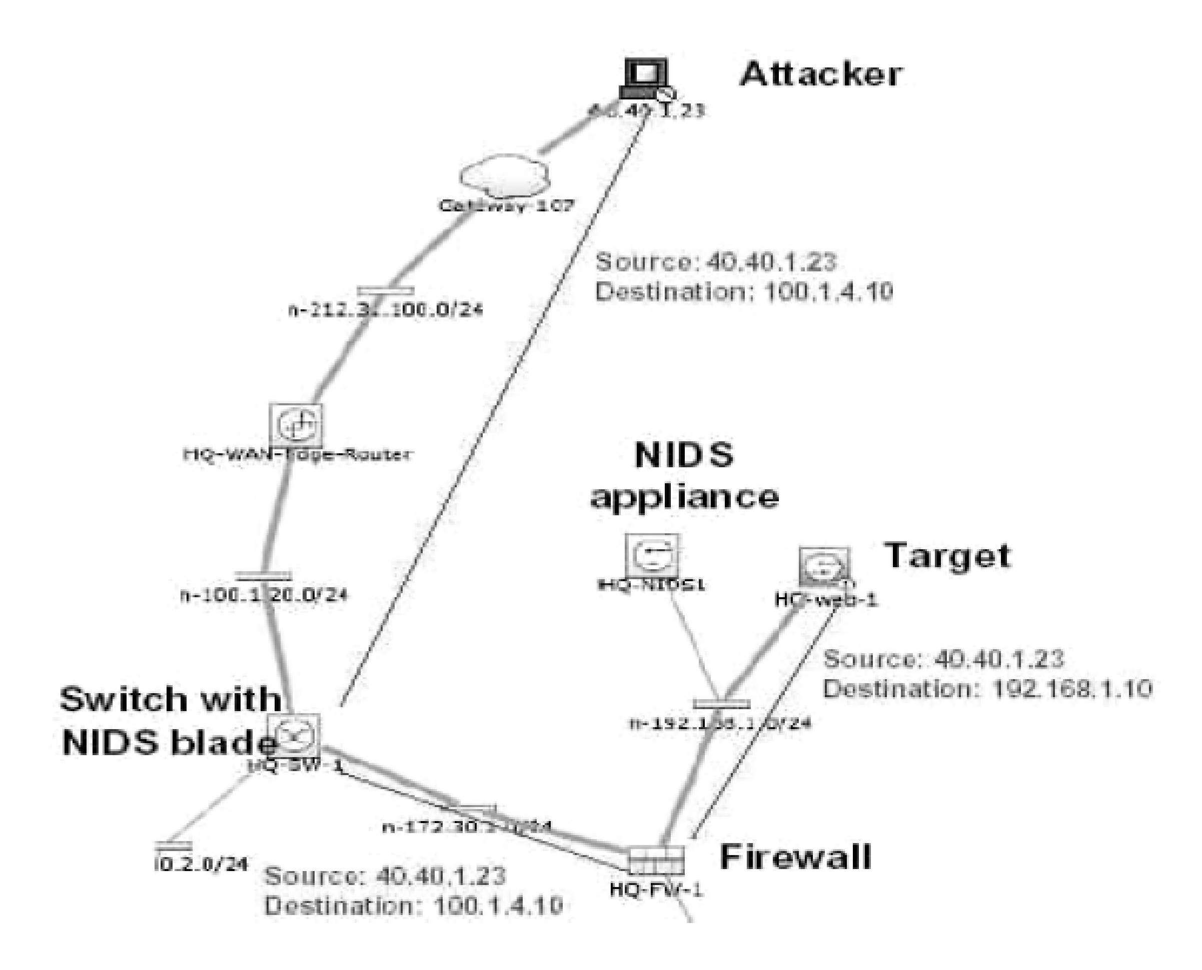


图 2-2 CS-MARS 显示的一个攻击事件

对于网络安全框架而言，最后一步就是作出相应的策略调整，在这一点上，CS-MARS也有独到之处，如图2-3和图2-4所示，它将自动生成对于安全事件的处理方法供网络管理

员实施。

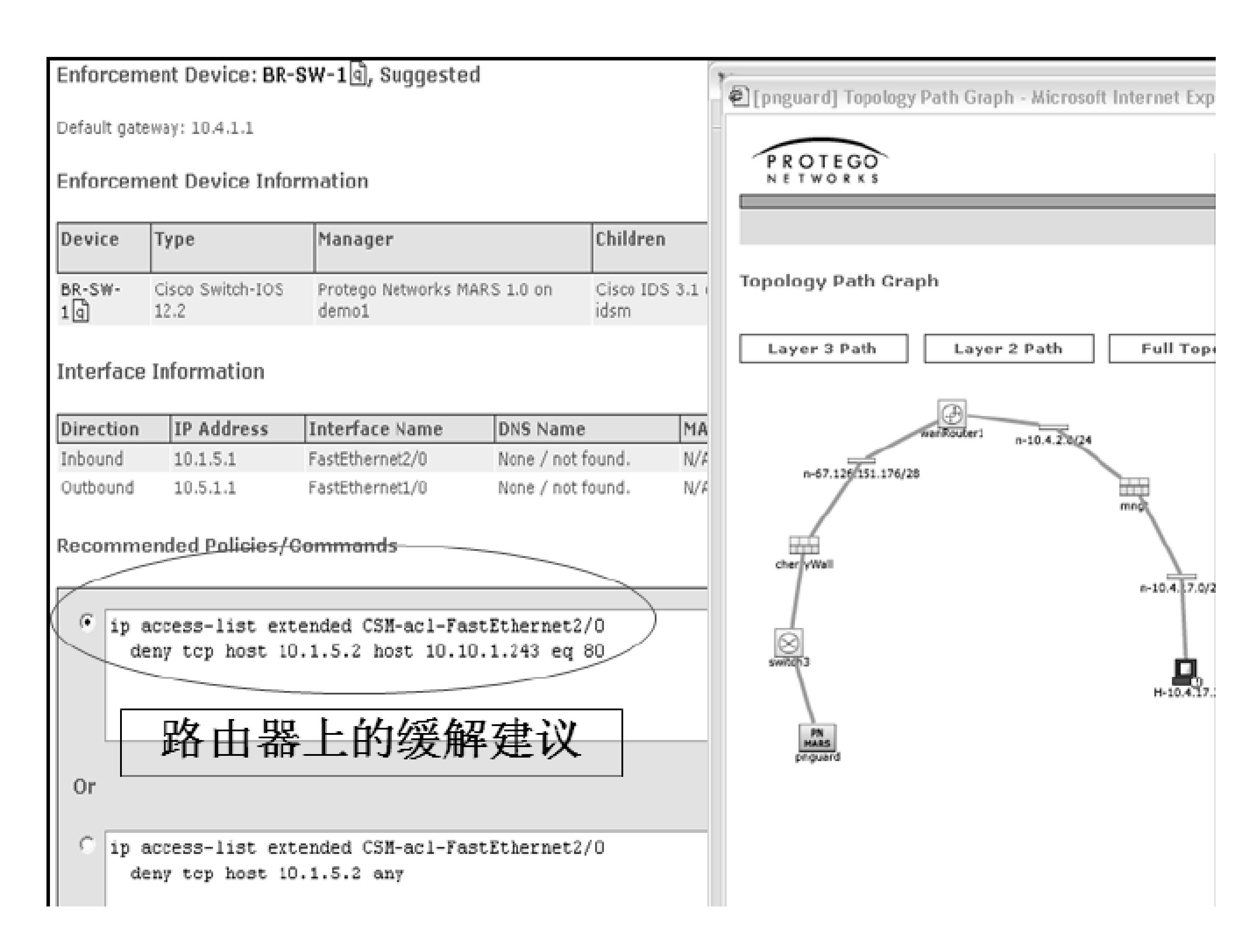


图 2-3　CS-MARS 显示解决方法 1

综上所述，对于整个安全框架而言，它围绕着安全策略分为四步，其过程如图 2-5 所示。

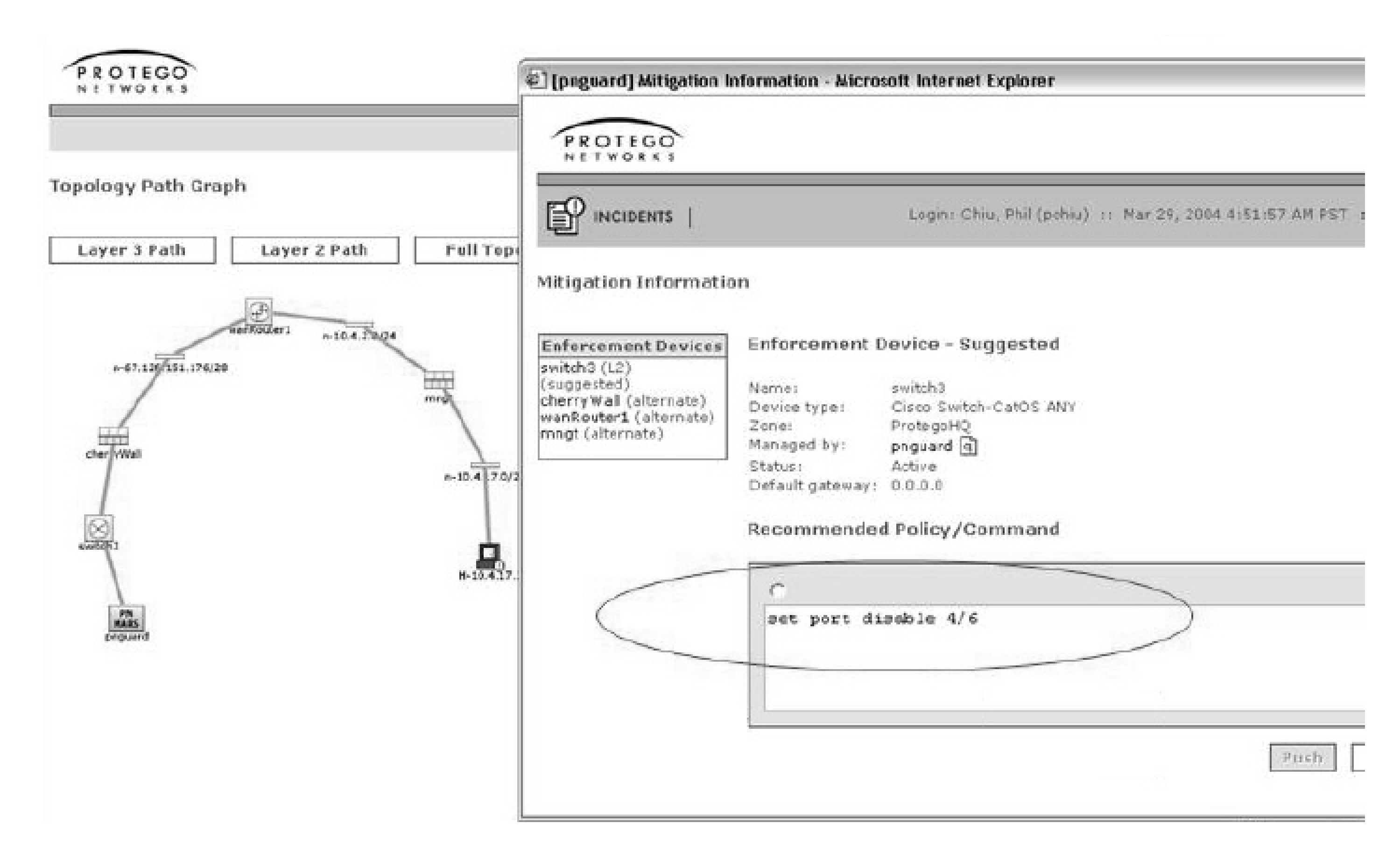


图 2-4　CS-MARS 显示解决方法 2

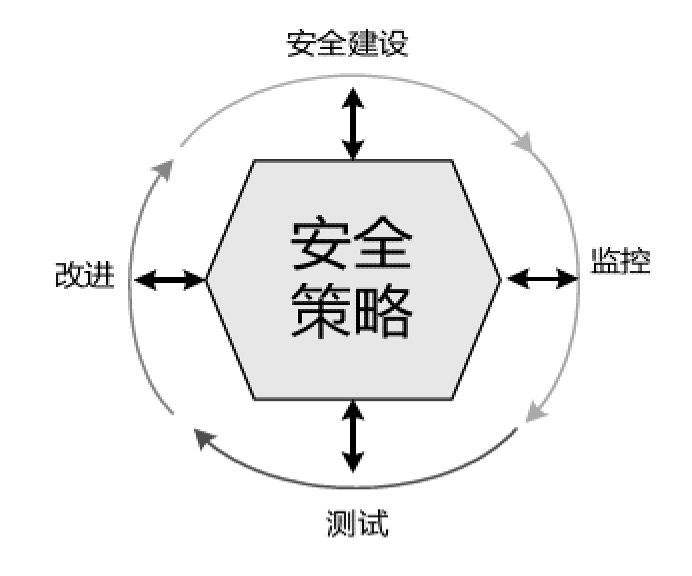


图 2-5　安全策略及安全框架

2.2 网络安全产品及解决方案

2.2.1 防火墙

我们已经熟知防火墙在网络中的作用，它就像一堵墙一样将威胁隔离在墙外，从而保证了内部关键网络的安全。按照使用环境可以分为个人防火墙和企业防火墙；按照架构又可以分为软件防火墙和硬件防火墙。软件防火墙主要有微软在 Windows XP 中加入的个人防火墙和用于较大规模网络的 ISA2004/2006 系列防火墙，当然还有 Symantec 的防火墙以及在 Linux 中的 Iptables 等。硬件防火墙主要由 Check Point、Cisco、Nortel、Nokia、NetScreen、天融信等公司提供。图 2-6 所示的是 Cisco 的 ASA 系列防火墙产品。



图 2-6 Cisco ASA 防火墙

在前面的章节中已经介绍了 DMZ 区域，如何创建 DMZ 区域，防火墙放置在网络中的什么位置成为一个十分关键的问题。如果 DMZ 区域设置不当，一方面可能导致防火墙根本无法有效地过滤流量；另一方面，正常的 VPN 远程接入由于防火墙防止不当而被阻隔，将会对公司业务带来非常大的影响。通常的 DMZ 区域分割采用三脚方式，如图 2-7 所示。

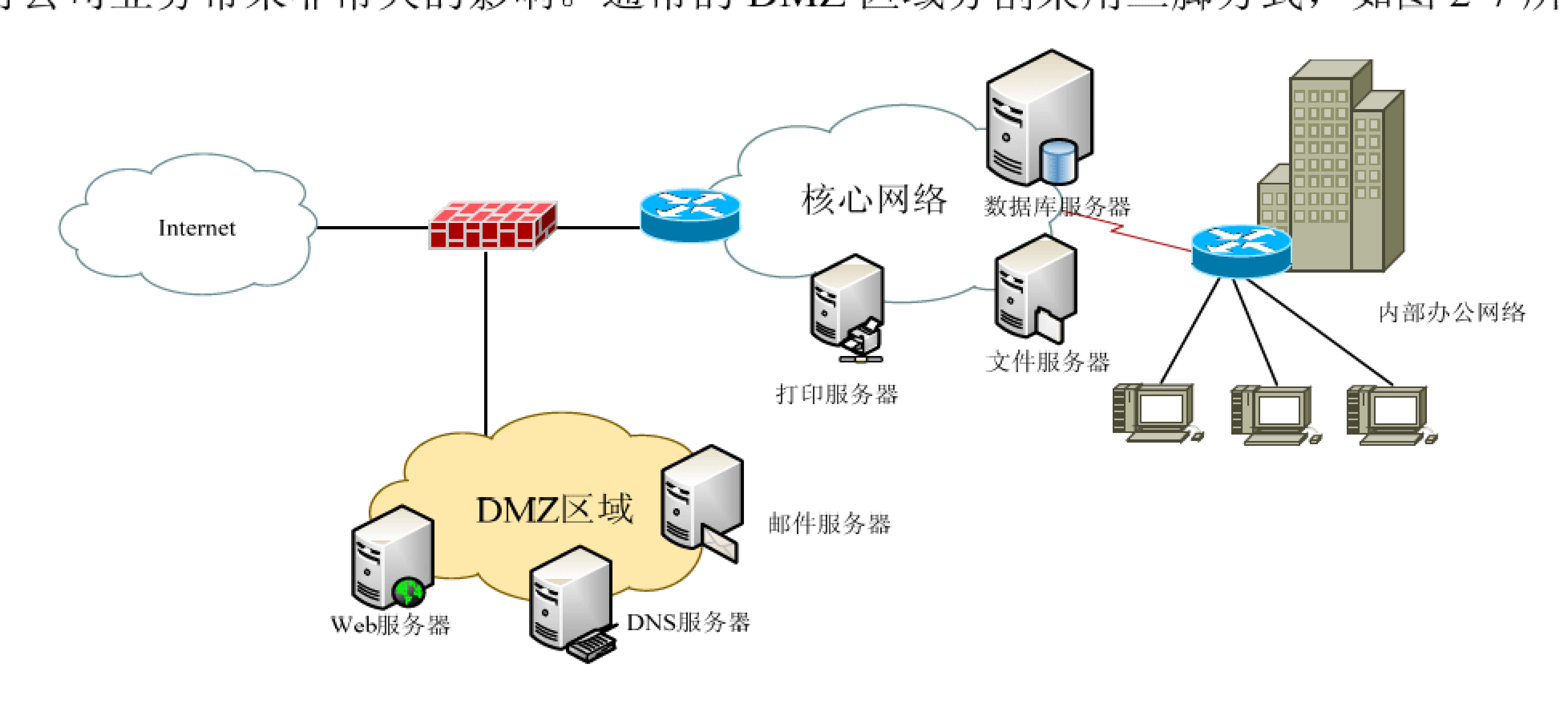


图 2-7 采用三角方式创建 DMZ 区域

当然有些时候，还可以根据 DMZ 区域内不同服务器的安全等级创建多个 DMZ，并且每个 DMZ 具有独特的安全特性。另一种方法是将 DMZ 区域完全放入公共网络，而防火墙仅做内外网隔离。例如在图 2-8 中，为了便于外网访问，将 Web 服务器放置在了防火墙外部，而 DNS 服务器、邮件服务器等仍然构成三脚形式的 DMZ 区域。

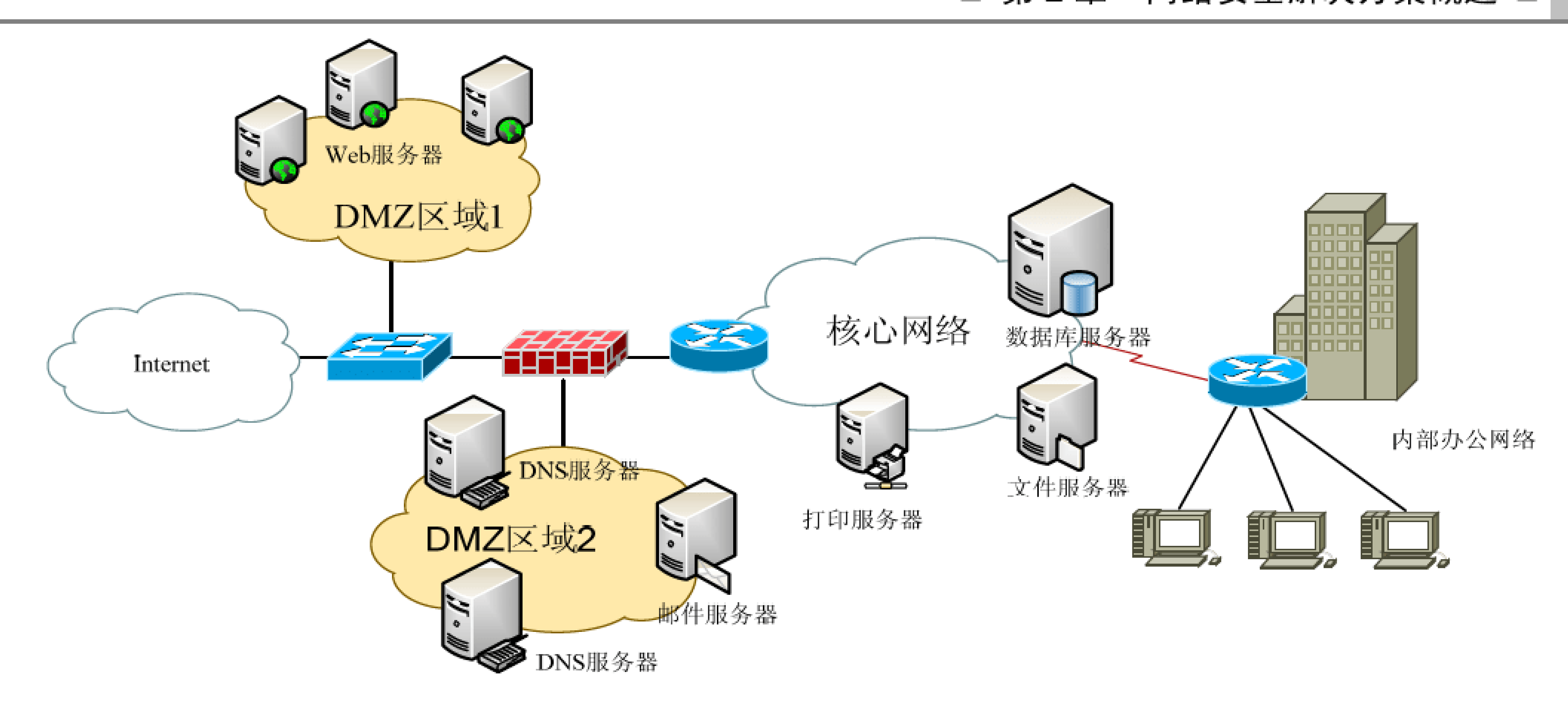


图 2-8　DMZ 区域放置在公共网络和防火墙之间

图 2-8 这种形式是一种错误的设计方式。这是因为，对于 DMZ 区域 1 而言，它根本未受到任何保护，仅能使用简单的访问控制列表来限制访问。从这种设计演化出了一种“脏 DMZ”的设计方案，脏 DMZ 的设计与图 2-7 十分相似，但是将图 2-8 中的交换机换成了一台路由器(如图 2-9 所示)。这样就可以很好地隔离了 DMZ 区域和内网之间的数据流量，同时前端路由器还可以分担部分流量，用于减轻对防火墙的攻击速度。

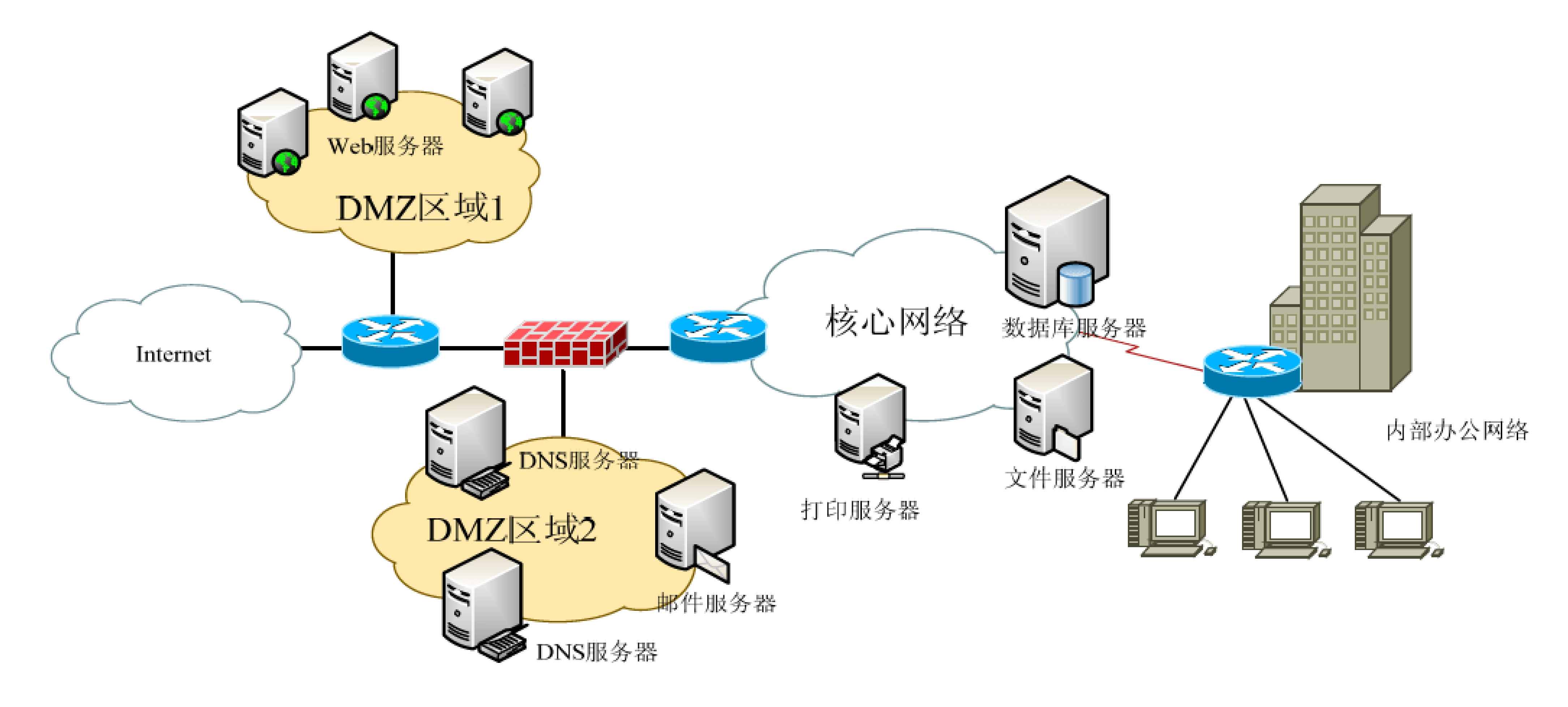


图 2-9　脏 DMZ

脏 DMZ 内放置的主机需要将不必要的设备全部关闭并及时安装补丁，构成能够应对网络攻击的堡垒主机，同时主机上开启大量的日志记录功能，捕获任何攻击企图，而且它还保证了壁垒主机被攻破后也无法成为传输重定向攻击的代理服务器。

最后，还有一种创建 DMZ 区域的方法是使用两个防火墙级联，将外网、DMZ 区域和内网完全隔离，这种方法相对于脏 DMZ 而言，堡垒主机的安全性进一步提高，同时也保证了内网和 DMZ 区域之间的隔离访问，如图 2-10 所示。但这种方法有一个缺点，就是所有内网的流量必须经过 DMZ 区域，则当 DMZ 区域有主机被攻陷后，流量很有可能被监听。

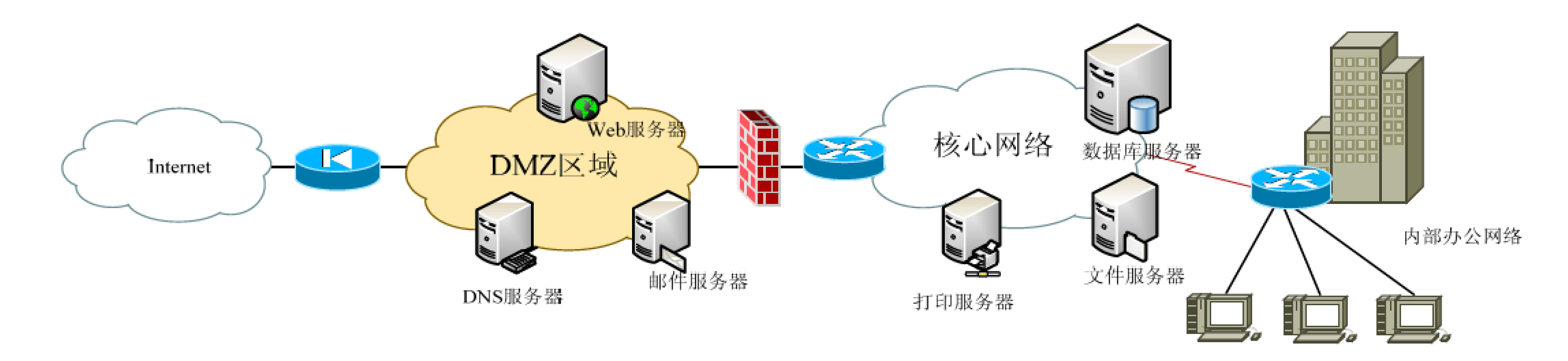


图 2-10 防火墙级联

2.2.2 VPN 接入

对于远程移动办公的用户可能需要 VPN 的接入服务以获得更安全的链接，但是我们同样会遇到一个难题，VPN 接入设备应该放置在什么地方？VPN 类型如何选择？

首先，我们来看 VPN 接入设备放置的位置。如果将其放置在防火墙后的内部网络，则防火墙过严的规则有可能限制了正常的 VPN 连接。 所以，一般来说 VPN 接入设备放置在防火墙外侧，如图 2-11 所示。

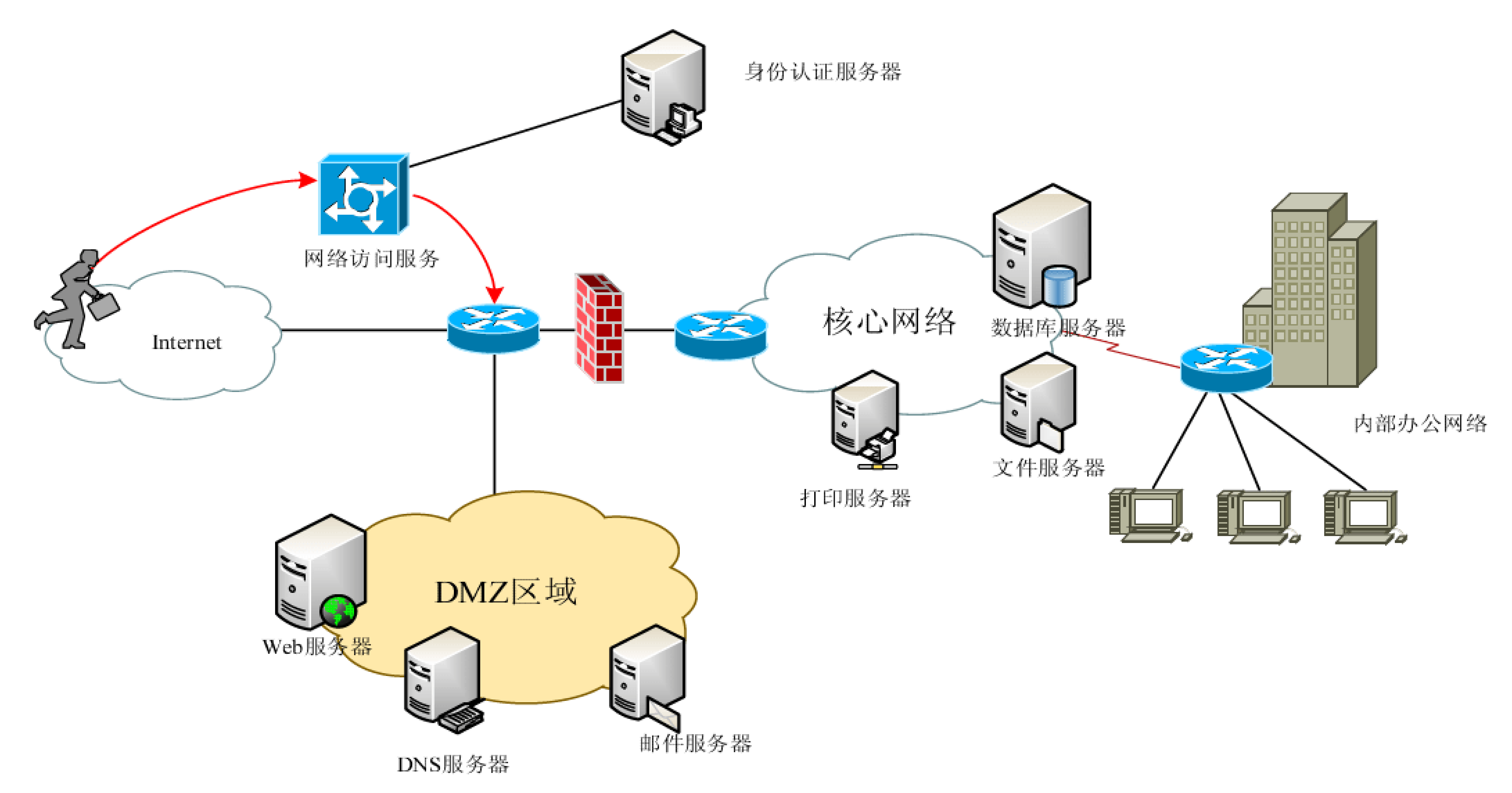


图 2-11 VPN 部署

为了访问安全，身份验证可以采用智能卡等多种形式进行。通常情况下，除了远程访问服务设备外，还有专门的 VPN 集中器产品，它可以用来进行远程办公室到本地办公室以及移动用户 IPSec、SSL VPN 拨入的身份验证工作。图 2-12 所示的是 Cisco VPN3000 集中器。



图 2-12　Cisco VPN3000 集中器

对于 VPN 类型，一般移动用户拨入采用 PPTP 协议或者 SSL VPN，而对于固定的站点到站点 VPN，通常使用 IPSec VPN。但随着 MPLS 的成熟，第二层 VPN 逐渐被用户所接受。Cisco 在其 PIX、ASA 防火墙产品以及部分路由器平台上也提供 VPN 拨入功能。

2.2.3　入侵检测

对于网络入侵，除了使用防火墙进行隔离外，对于关键的服务器还需要进行更多的防护机制。IDS 就是这样的设备，它用于对入侵进行监控和响应。同样 IDS 也有很多厂商生产，由于网络中通常需要部署多个 IDS，Cisco 在其路由器平台上增添了 IOS IDS 功能的同时，还同时生产独立的 IDS 设备以及交换机上的 IDS 模块。图 2-13 所示的是 Cisco 4200 系列入侵探测器。



图 2-13　Cisco 4200 系列入侵探测器

早期的 IDS 系统通过查找任何异常的通信发挥作用。当检测到异常的通信时，这种行动将被记录下来并且向管理员发出警报。这个过程很少出现问题。开始时，查找异常通信会产生很多错误的报告。经过一段时间之后，管理员会对收到过多的错误警报感到厌烦，从而完全忽略 IDS 系统的警报。

比较新的 IDS 系统比以前的系统更准确一些。但是，这个数据库需要不断地更新以保持有效性。而且，如果发生了攻击并且在数据库中没有相匹配的特征码，这个攻击可能就会被忽略。即使这个攻击被检测到了并且被证实是一种攻击，IDS 系统除了向管理员发出警报和记录这个攻击之外没有力量做任何事情。

Cisco 在原有 IDS 硬件平台上开发了 IPS 系列入侵防御系统。IPS 位于防火墙和网络的设备之间。这样，如果检测到攻击，IPS 会在这种攻击扩散到网络的其他地方之前阻止这个恶意的通信。相比之下，IDS 只是存在于内部网络之外起到报警作用，而不是在内部网络前面起到防御作用。

IPS 检测攻击的方法也与 IDS 不同。目前有很多种 IPS 系统，它们使用的技术都不相同。

但是，一般来说，IPS 系统都依靠对数据包的检测。IPS 将检查入网的数据包，确定数据包的真正用途，然后决定是否允许数据包进入内部网络。

IDS/IPS 在网络中放置的位置也是值得我们关注的。通常上述的 IDS/IPS 为网络型，它们用于监控一系列地址段的通信安全，但 IDS、IPS 大多是基于 x86 结构的 Linux 系统，检测导致其吞吐量并不大。所以放置时应当采用按需放置的原则，通常是放置在防火墙之后，关键服务器之前的位置，如果放置在防火墙之前，将会产生大量的攻击信息警报送到监控系统，而最终很多攻击又被防火墙拦截。实际放置方式如图 2-14 所示。

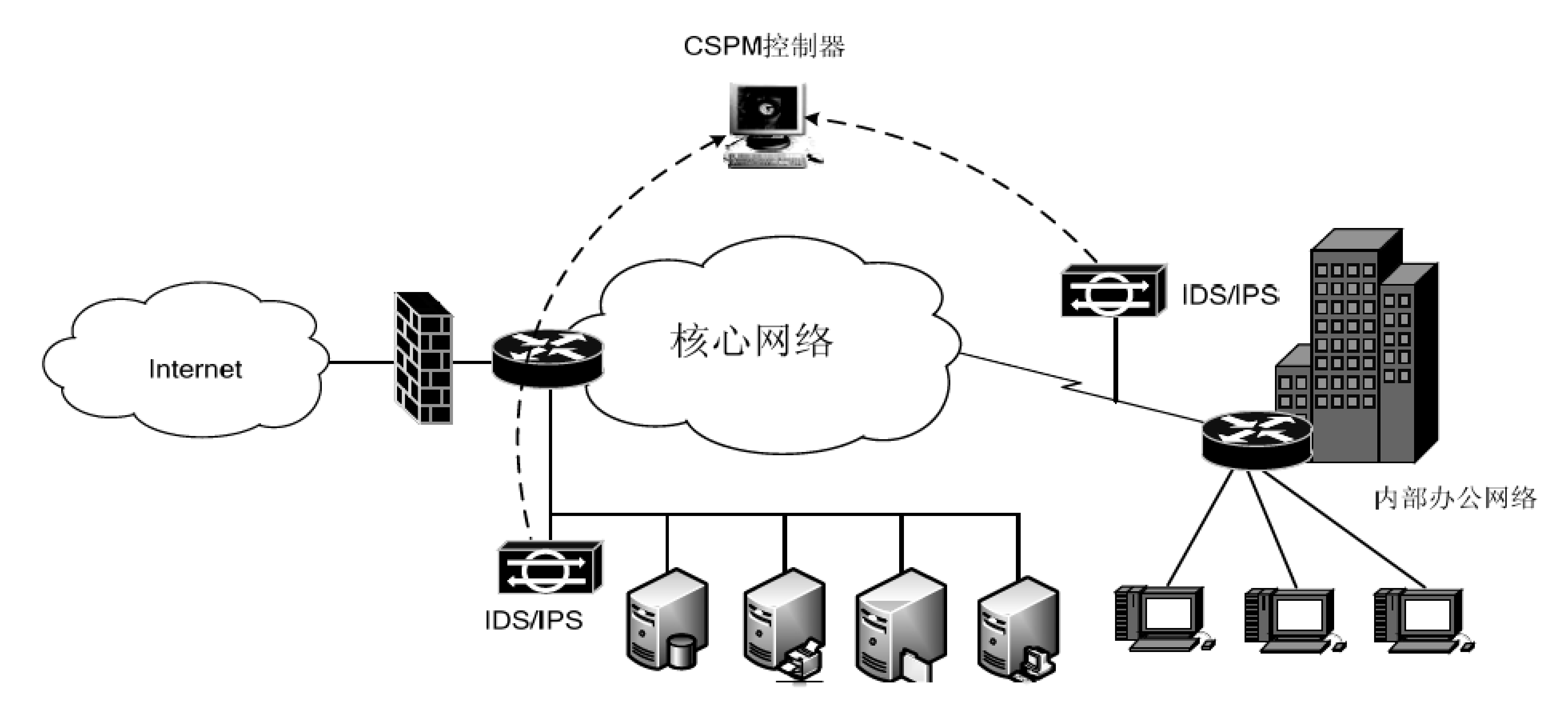


图 2-14　IPS/IDS 放置方式

2.2.4　集成安全设备

有时候为了节省成本和机架空间，以及从供电、散热等方面考虑。我们可以将防火墙、IDS 等设备集成到路由器和交换机中。最常见的是基于 IOS 系统的 IDS/IP 以及 IOS 防火墙。在 6500 系列交换机上还有 VPN 模块(如图 2-15 所示)、IDS 模块(如图 2-16 所示)及 NAM 网络分析模块等，极大地简化了部署难度。

同时，Cisco 还提供了 ISR 集成多业务路由器，用于分支机构和中小型企业。通过功能的集成，在提供较好安全性的同时，也降低了成本。当然对于一些更小型的企业而言，可能也没有足够的经费投资到网络安全建设上，因此稍后的章节我们将为大家介绍一些基于 Linux 的廉价网络安全方案。

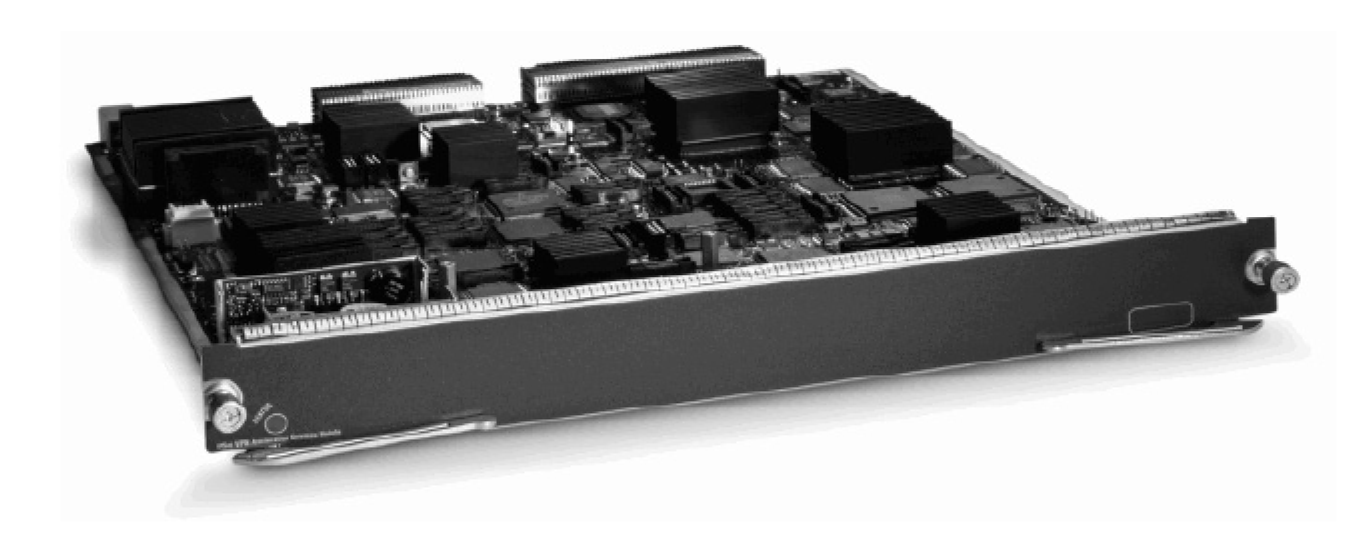


图 2-15　VPN 模块

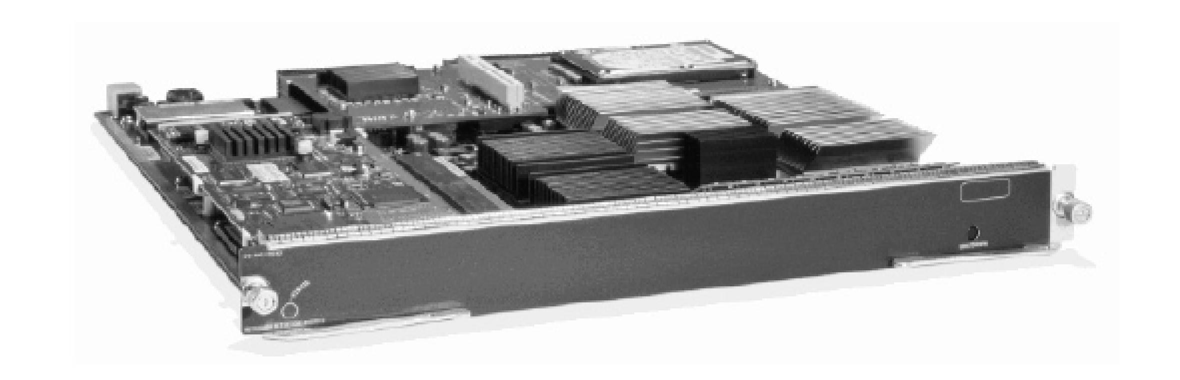


图 2-16　IDS 模块

2.2.5　DDoS 检测和防范

DDoS(Distributed Denial of Service，分布式拒绝服务)攻击由于触发过程简单，同时产生的影响巨大，随着服务提供商、企业和政府机关对因特网依赖的加剧，使得成功的 DDoS 攻击能造成更加严重的破坏(经济和其他方面)。最近，又出现了更多功能更为强大的 DDoS 工具，使得将来的攻击破坏性更大。DDoS 已经成为当今网络威胁的主要来源，如何防止 DDoS 攻击成为我们所关注的焦点。而且 DDoS 攻击以及出现集团化犯罪趋势，根据最近的资料显示，我国已经破获了一些 DDoS 犯罪团伙。

传统的 DDoS 防治建立在主机上，但是大量的 DDoS 攻击也会非常容易导致主机崩溃，而放置 IDS/IPS 的网络也无法及时地对攻击流量进行响应。例如 Sina 的 UC 聊天室，流量通常情况下为 100Mbps，而每天的攻击流量大于 500Mbps。当一个运营商的 10G 互联骨干上，带宽有可能被瞬间填满。这些带着极大利益趋势的攻击行为逐渐演变为一种犯罪机制，而产生这样的攻击流量在国内仅需 100 元人民币就可以获得。图 2-17 是 Symantec 提供的 DDoS 攻击数据。

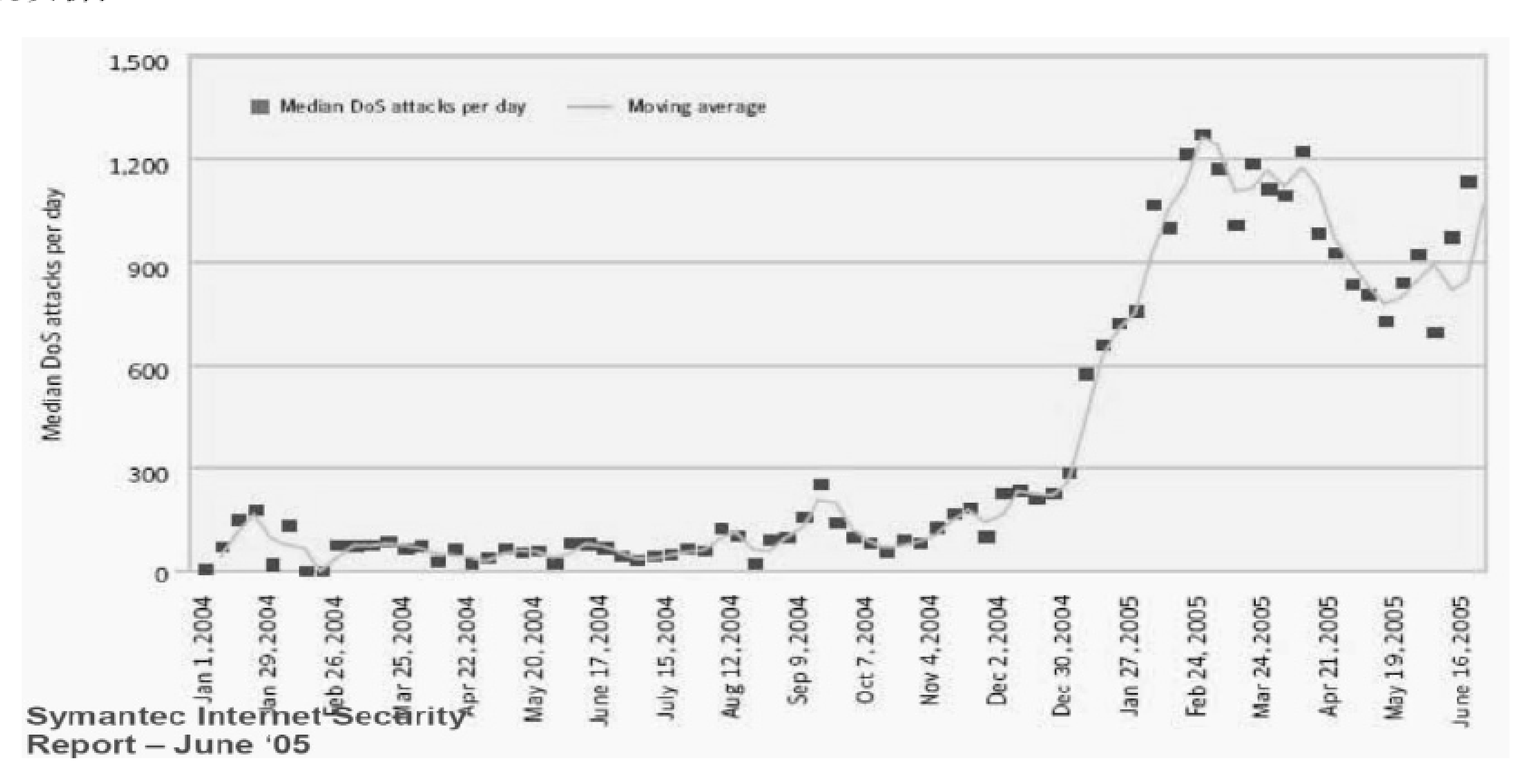


图 2-17　DDoS 攻击统计数据

因此在整个网络上，特别是运营商网络上进行专门的 DDoS 防范非常有必要。Cisco 在这一领域带来了非常值得借鉴的解决方案。它提供了 DDoS Anomaly Guard 和 DDoS Traffic Anomaly Detector 两种设备用于防止 DDoS 攻击，同时在产品上提供 Catalyst 6500 系列交换机和 7600 路由器使用的服务模块，还提供了基于 IBM X345、X356 服务器的外置解决方案，如图 2-18 所示。



图 2-18　DDoS Guard 产品

除此之外，还可以通过使用 Arbor Networks Peakflow SP 统计路由器的 Netflow 流量为 Anomaly Guard 提供检测依据，如图 2-19 所示。



图 2-19　Peakflow SP

图 2-20 所示的是 DDoS Guard 常用的部署方式。

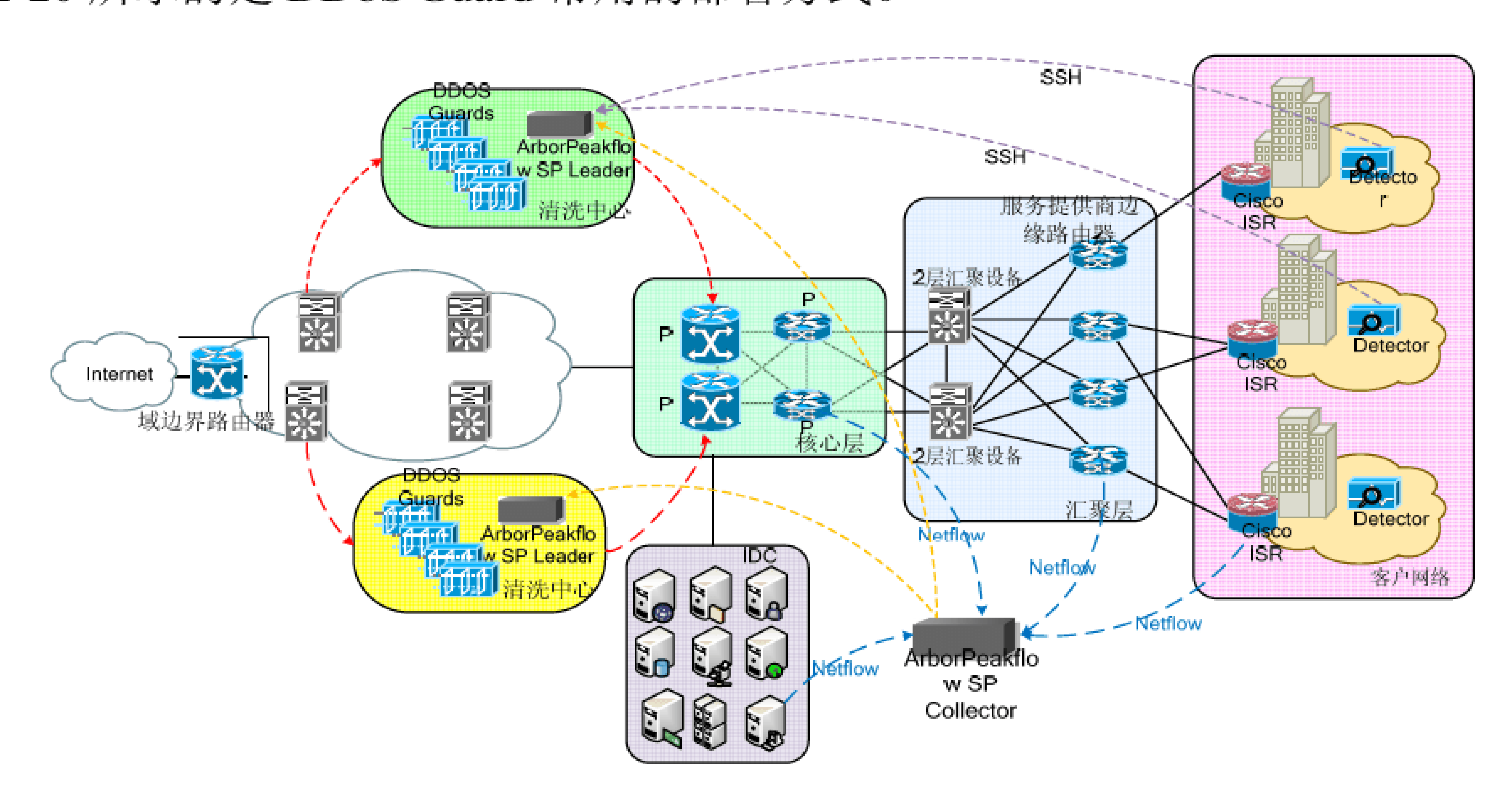


图 2-20　DDoS Guard 部署

2.2.6　CSA 与 NAC

在整个网络中，关键服务器及员工电脑的病毒防护也值得我们关注。带病毒的计算机连入网络后将在内部网络造成病毒泛滥，这样带来的威胁比外部威胁更大。特别是文件服务器等带有病毒后，随着文件的分发将会导致全网中毒。

CSA(Cisco Security Agent，Cisco 安全代理)是一种安全代理软件，它通过一系列特有的标准用于评判一台主机是否安全。它可以很好地保护服务器不受攻击，即便受到攻击后也可以通过 CSA 及时地将带毒日志发送到管理服务器上。而对于 NAC(Network Admission

Control，网络接入控制)，它则是配合 CSA 的一种网络接入控制机制，当员工电脑尚未完成系统升级和杀毒软件更新的情况下，它将隔离用户的网络访问，使其只能访问到病毒更新服务器和系统更新服务器，当更新完成并且 CSA 评估为安全后，方能连上网络。图 2-21 所示的是 CSA 安全代理软件的控制界面。

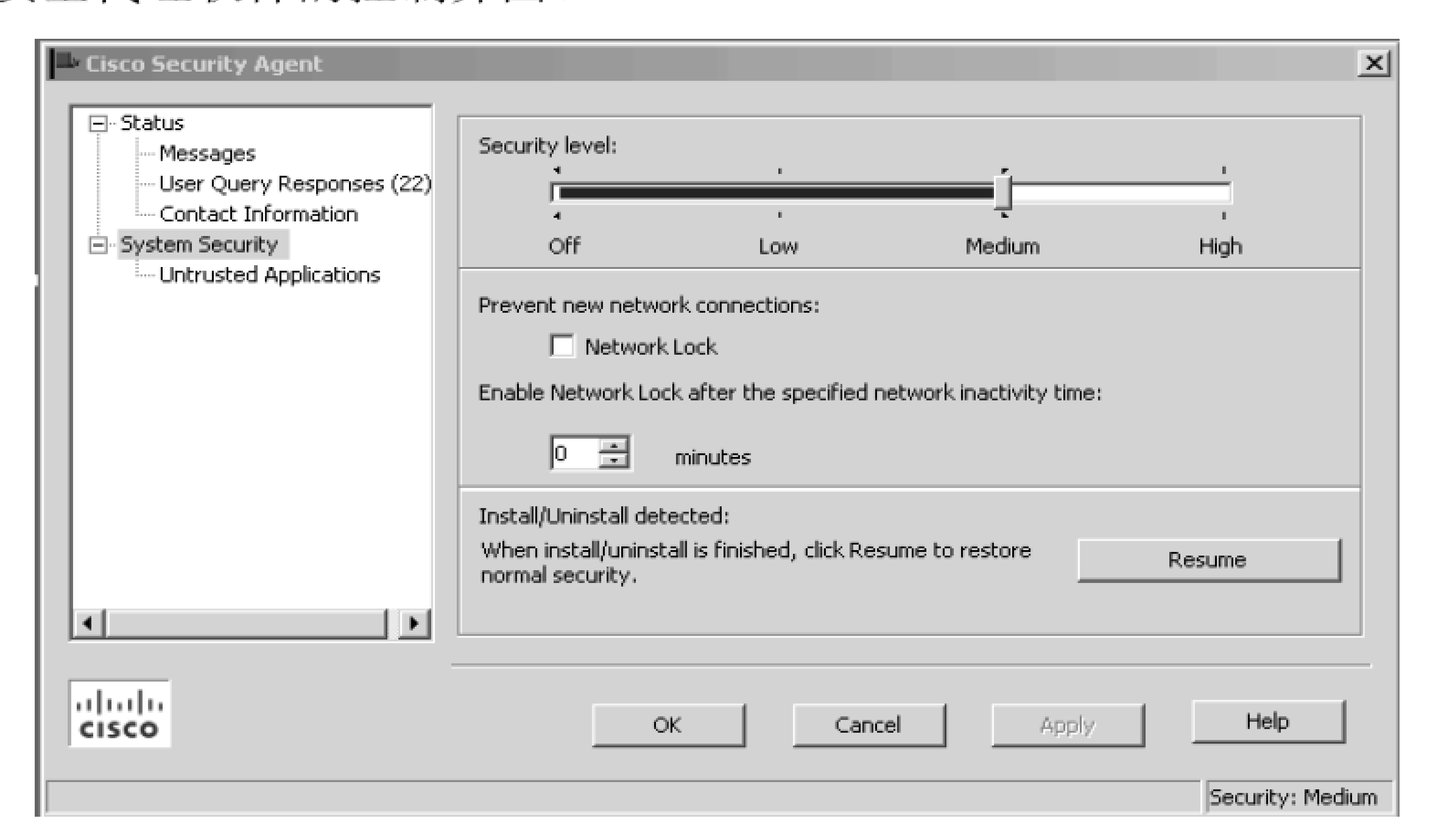


图 2-21　CSA 安全代理

2.2.7　网络安全设备联动

我们在网络中可能会部署很多安全设备，并且产生大量的安全日志。如何管理这些日志并作出全局上最快的、最佳的响应也是我们需要关注的问题。同时，所有网络安全设备的联动使得网络安全性获得极大的提高，Cisco 在这方面提供了检测分析响应设备 CS-MARS(Cisco Security Monitoring, Analysis and Response System， Cisco 安全监控、分析和响应系统)，如图 2-22 所示。



图 2-22　CS-MARS

CS-MARS 可以支持众多设备的安全信息收集，例如路由器、IDS、IPS、ASA 等产品。同时，CSA 以及一些第三方的安全软件也都可以加入 CS-MARS 中，并且 CS-MARS 可以对它们产生的大量日志作出面向整个网络的可视化攻击分析。图 2-23 所示的是 CS-MARS 生成的网络拓扑。

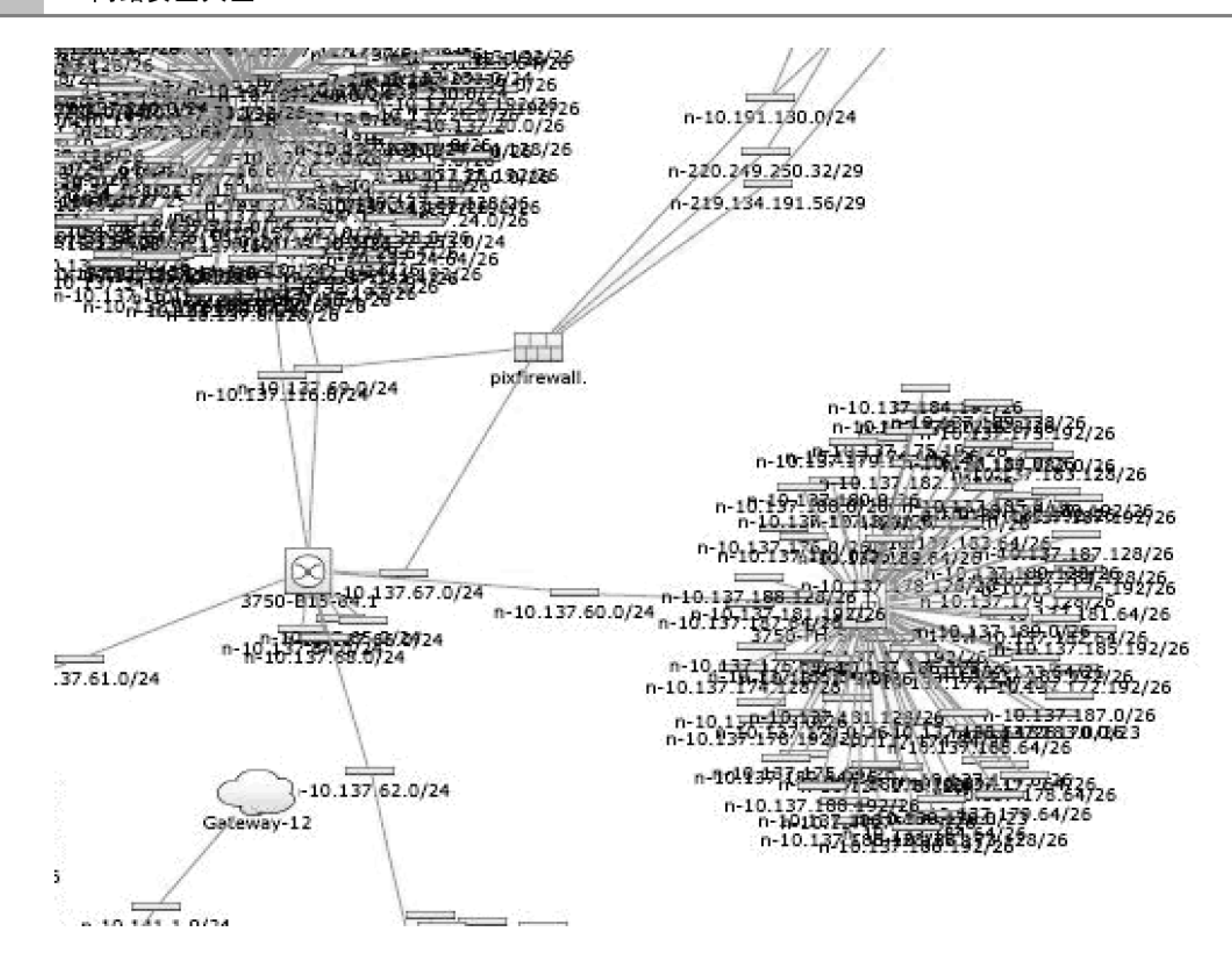


图 2-23　CS-MARS 生成的网络拓扑

2.3　本 章 小 结

这一章我们介绍了一些常见的网络安全解决方案，并且对于如何部署网络安全解决方案做了一些简单的介绍。通过这一章的学习，可以使我们懂得如何建立一个安全的网络系统，并且对于常见的攻击行为进行快速的响应。

第 3 章　网络设备安全

本章将从三个不同的方面讨论网络设备的安全问题。首先讨论网络设备的物理安全，包括供电安全、环境安全等；接着讨论各种网络设备的访问权限及相应的漏洞攻击和防范方法等，并且详细介绍了一些网络冗余协议和实施方案；最后介绍了一些访问控制列表的使用方法，并用其来构造一个简单的网络访问控制方案。

通过本章的学习，读者应掌握以下主要内容：

✧ 网络设备物理安全
✧ 网络设备冗余
✧ HSRP 等网络冗余协议
✧ 网络设备安全配置
✧ SNMP 日志服务

3.1　网络设备的物理安全

应用实例导航：UT 大学城网络设备物理安全设计

※场景呈现

UT 大学城园区网络最初采用 3 层结构(即核心层、分发层和接入层)设计。有一次核心机房断电，由于 UPS 长期没有监控，电池已经失效，同时输出功率无法满足所有设备的同时启动，这次意外断电导致大量的用户网络中断。对于这样一个网络结构，网络管理员无论做多少逻辑层面上的安全防范也永远敌不过一个黑客(或许就是一个普通的人关掉核心机房供电)。

后期 UT 大学城在网络改造的过程中考虑到这些因素，开始定期对 UPS 进行检查，并将 UPS 监控系统整合到整个网络管理系统中，还根据一些扁平式网络设计，分散了核心网络结构，如图 3-1 所示。

※技术要领

(1)　网络设备物理安全的基本概念；
(2)　网络设备冗余的配置方法；
(3)　网络设备异常的及时检测方法。

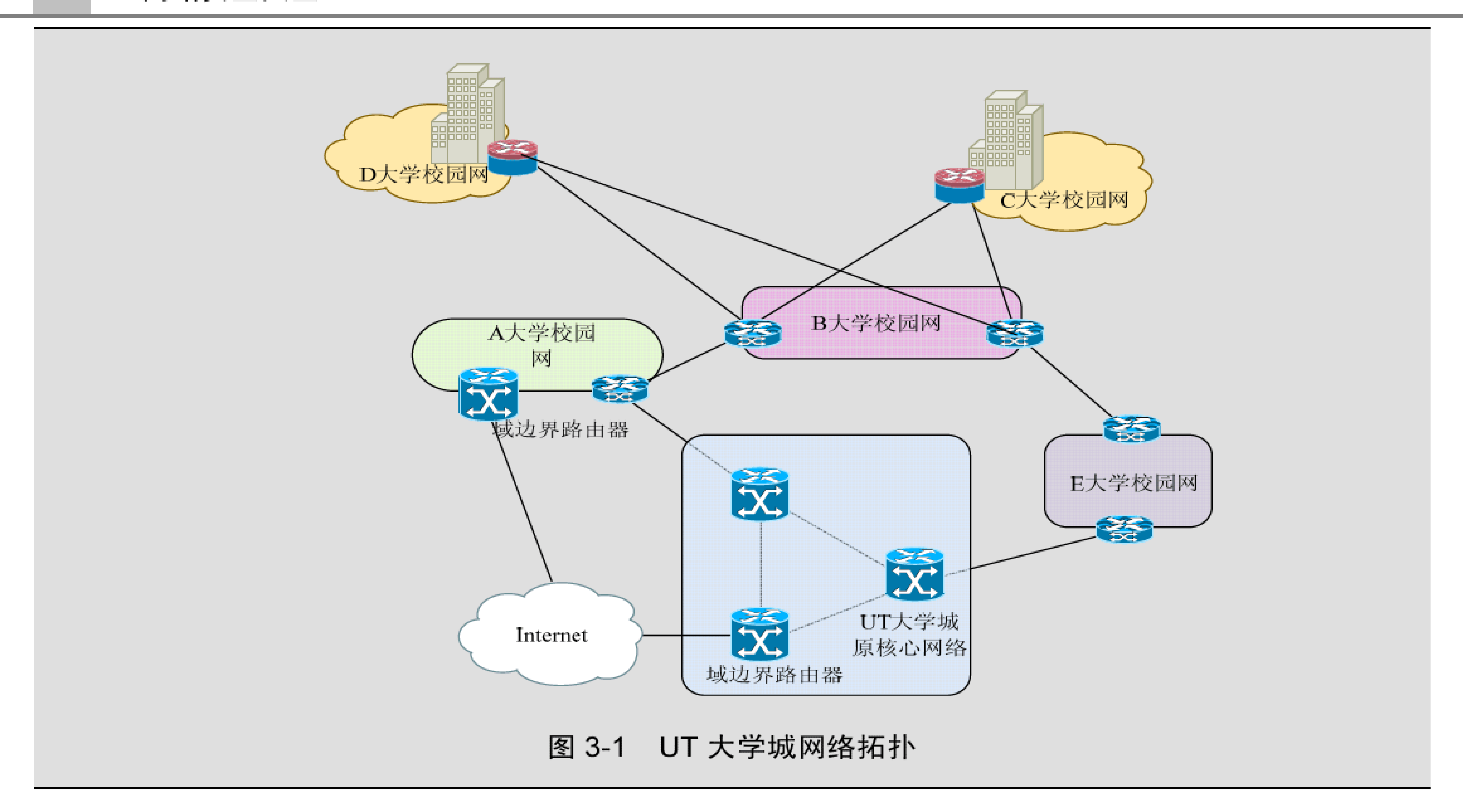


图 3-1　UT 大学城网络拓扑

就图 3-1 所示的拓扑图而言，每个校区都保证了双线接入，包括 Internet 的出口也是双链路备份的，看上去已经相当的稳定了。但是某日，B 校区由于配电设备改造，需停电 20 小时，而 B 校区机房 UPS 仅能支持 4 小时，并且没有配置发电设备，断电后另外几个校区将会出现无法访问网络的状况，如图 3-2 所示。

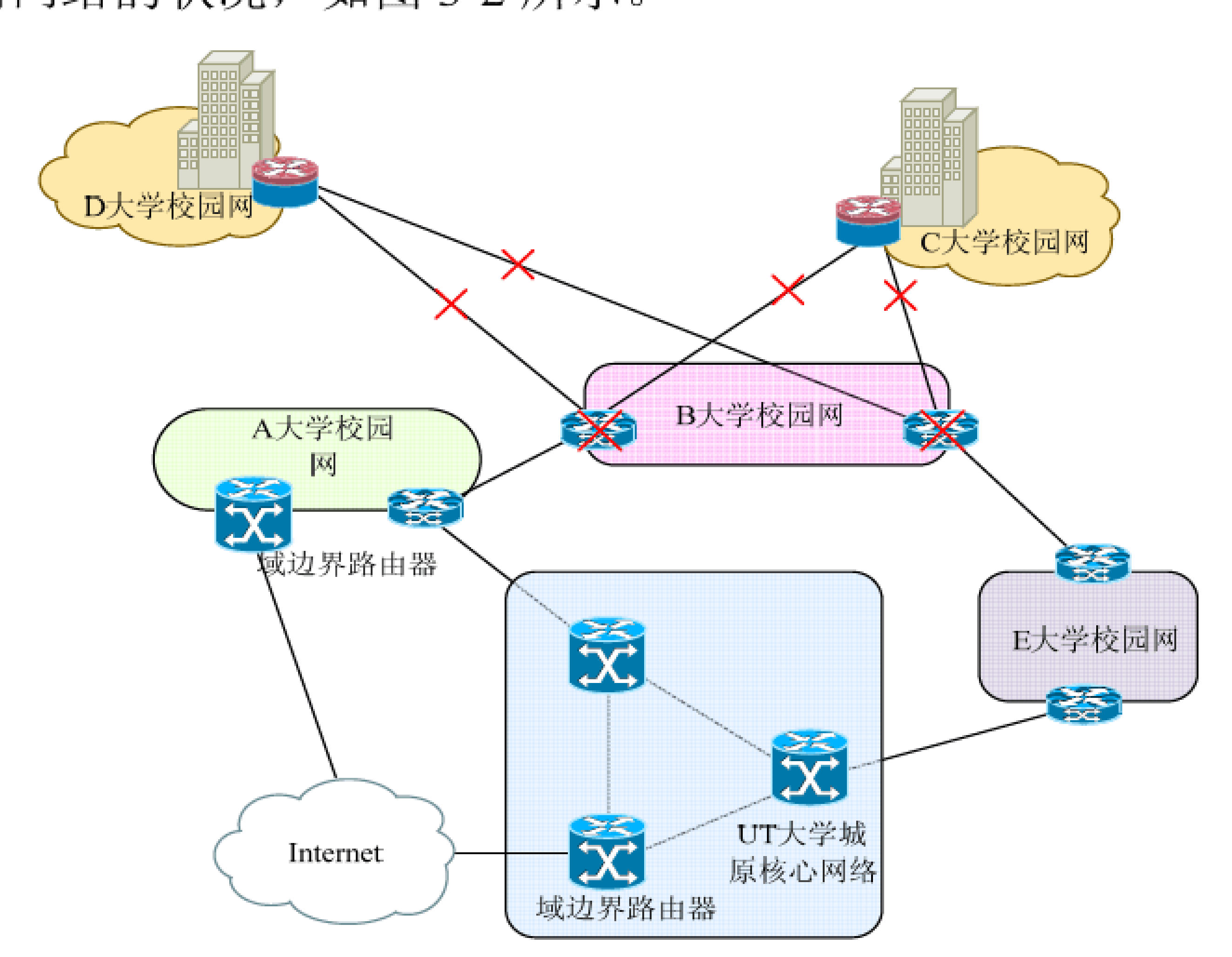


图 3-2　UT 大学城故障网络拓扑

因此，在设计网络时，冗余链路备份也需要进行良好的设计才能保证网络的安全运行。在必要的情况下，除了使用热备份协议外，还应当使用适当的冷备份设备。

对于机房选址而言，需要物理位置足够分散，能够确保自然灾害对其影响较小，供电应当保持稳定。在条件许可的情况下，应配置双电源切换和长时间 UPS 保护。同时，要加

强机房的安全控制，对于一栋楼而言，机房应该设置在相对隔离的位置，这样就能防止不必要的物理入侵。与此同时，机房入口和布线室应采用摄像监控。

同样，在连接交换机的时候，很多情况下都有两条链路进行备份，例如在图 3-1 所示的各个校区，很多用户喜欢把两条上行链路连接到同一个引擎上，如图 3-3 所示。

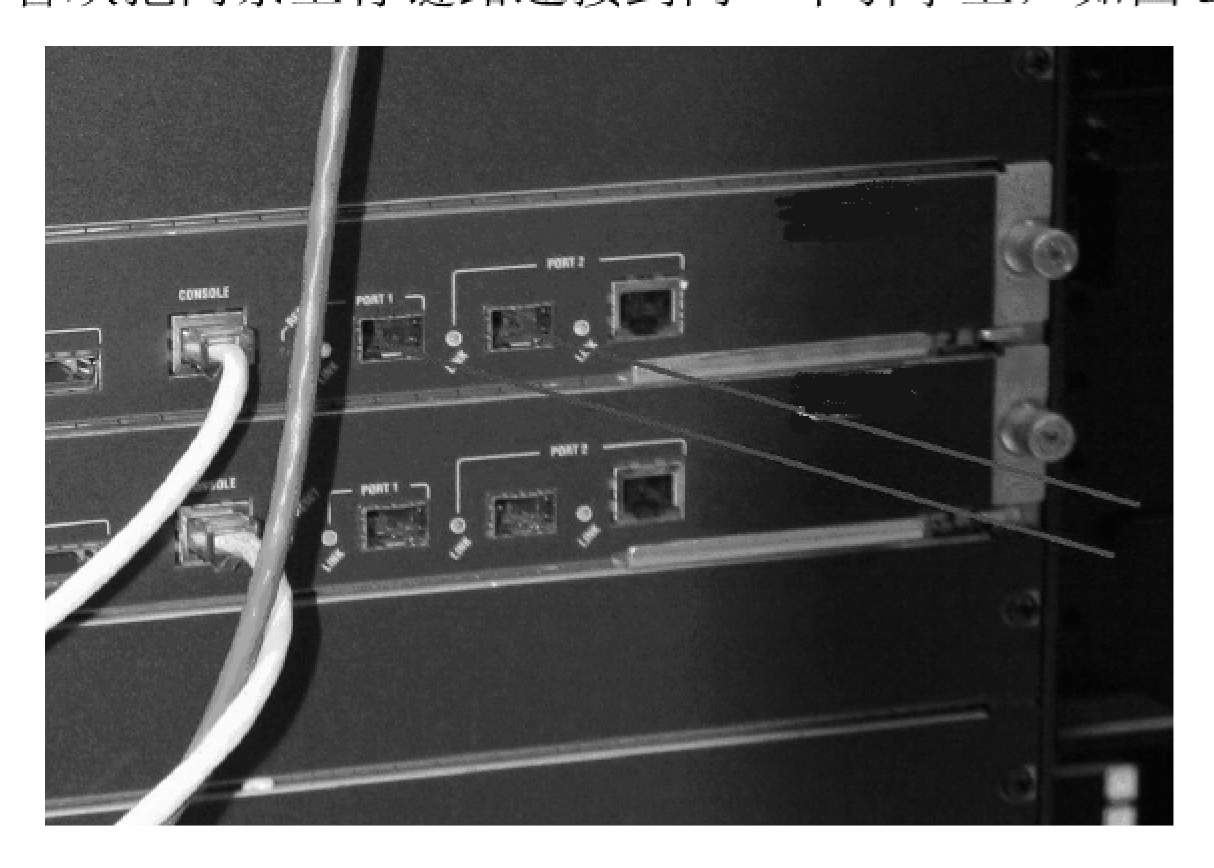


图 3-3　将两条上行链路连接到同一个引擎

正确的做法是，将两条上行链路连接到不同的引擎上，这样当某一块引擎出现故障的时候，交换机依旧可以正常工作，对稳定性的提升也十分明显，如图 3-4 所示。

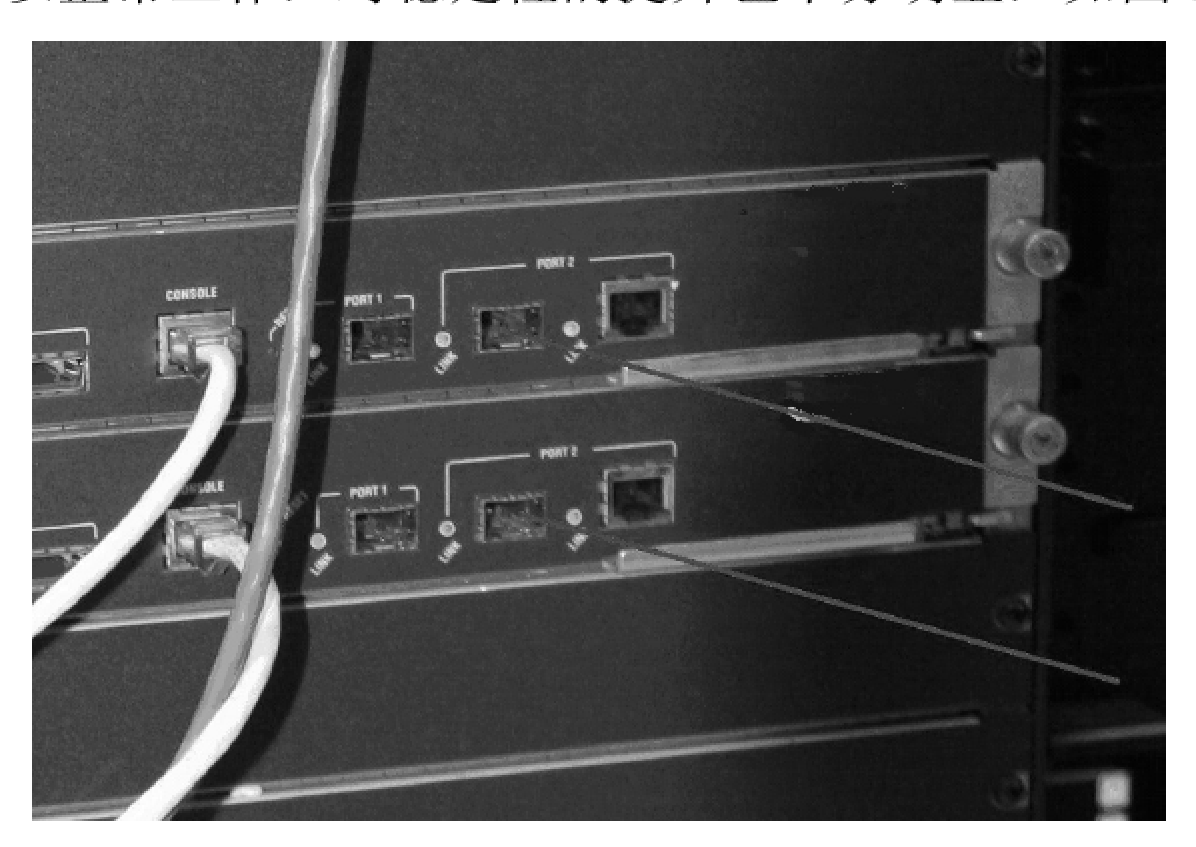


图 3-4　将两条上行链路连接到不同的引擎

3.2　网络设备冗余

3.2.1　HSRP 简介

HSRP(Hot-Standby Router Protocol)主要用于路由器热备份。实现 HSRP 的条件是网络系统中有多台路由器，它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任一时刻，一个组内只有一个路由器是活动的，并由它来转发数据包，如果活动路由器发生了故障，

将选择一个备份路由器来替代活动路由器，但是在内部网络的主机看来，虚拟路由器没有改变。当一台路由器发生故障时，主机仍然保持连接，不会受到故障的影响，这样就较好地解决了路由器切换的问题。

为了减少网络的数据流量，在设置活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送 HSRP 报文。如果活动路由器失效，备份路由器将接管成为活动路由器。如果备份路由器失效或者变成了活动路由器，将有另外的路由器被选为备份路由器。

在一个特定的局域网中，可能有多个热备份组并存或重叠。每个热备份组模仿一个虚拟路由器工作，它有一个 Well-known-MAC 地址和一个 IP 地址。该 IP 地址、组内路由器的接口地址、主机在同一个子网内，但是不能一样。当在一个局域网上有多个热备份组存在时，把主机分布到不同的热备份组，可以使负载得到分担。

3.2.2 HSRP 工作原理

HSRP 利用一个优先级方案来决定哪个配置了 HSRP 的路由器成为默认的主动路由器。如果一个路由器的优先级设置得比所有其他路由器的优先级高，则该路由器成为主动路由器。路由器的默认优先级是 100，所以如果只设置一个路由器的优先级高于 100，则该路由器将成为主动路由器。

通过在设置了 HSRP 的路由器之间广播 HSRP 优先级，HSRP 将选出当前的主动路由器。当在预先设置优先级的一段时间内主动路由器不能发送 Hello 消息时，优先级最高的备用路由器变为主动路由器。路由器之间的包传输对网络上的所有主机来说都是透明的。

配置了 HSRP 的路由器交换以下三种多点广播消息。

✧ Hello——Hello 消息向其他路由器发送路由器的 HSRP 优先级和状态信息，HSRP 路由器默认为每 3 秒钟发送一个 Hello 消息。
✧ Coup——当一个备用路由器变为一个主动路由器时发送一个 Coup 消息。
✧ Resign——当主动路由器要停机或者当有优先级更高的路由器发送 Hello 消息时，主动路由器发送一个 Resign 消息。

在任何时刻，配置了 HSRP 的路由器都将处于以下六种状态之一。

✧ Initial——HSRP 启动时的状态，HSRP 还没有运行，一般是在改变配置或端口刚刚启动会进入该状态。
✧ Learn——路由器已经得到了虚拟 IP 地址，但是它既不是活动路由器也不是等待路由器，它一直监听从活动路由器和等待路由器发来的 Hello 消息。
✧ Listen——路由器正在监听 Hello 消息。
✧ Speak——该状态下路由器定期发送 Hello 消息，并且积极参加活动路由器或等待路由器的竞选。
✧ Standby——当主动路由器失效时路由器准备接包传输功能。
✧ Active——路由器执行包传输功能。

使用 HSRP 时，当末端工作站使用的默认网关不可用时，可以继续在网络上进行通信。在 HSRP 中采用了一套路由器，分为活跃、备份、虚拟、其他路由器等体系，在外部看来，它是一台拥有 IP 和 MAC 地址的目标路由器。

活跃路由器的功能是负责转发发送到虚拟路由器的数据，它通过发送 Hello 消息(基于 UDP 广播)来通告它的活跃状态组中会有另外一台路由器作为备份路由器。备份路由器的功能是监视 HSRP 组中的运行状态，并且在当前活跃路由器不可用时，迅速承担数据转发的任务。备份路由器也发送 Hello 消息向组中其他的路由器通告其备份路由器的角色。

虚拟路由器的功能是向最终用户代表一台能持续工作的路由器设备。虚拟路由器有自己的 MAC 和 IP 地址，但是实际上它不转发数据包，仅仅是代表一台可用的路由设备。若网络中还有其他路由器，它们也能监听到 Hello 消息，但是不作应答，这样它们就不会在备份组有身份的概念，同时它也不参与发送到虚拟路由器的数据包，但是还是转发其他路由器发来的数据包。

下面所列的是活跃路由器选择的方法。

- ✧ 在 HSRP 中，有最高备份优先级的路由器将成为活跃/备份路由器，默认的优先级是 100，优先级范围是 0～255。
- ✧ 当优先级相同的情况下，具有最高 IP 地址的路由器将成为活跃路由器。
- ✧ 默认 MAC 地址最小的成为活跃路由器。

3.2.3 配置 HSRP

下面简要介绍 HSRP 的基本配置。

❶ 配置一个路由器接口(物理接口或虚拟接口)，让其参与 HSRP 备份组。

```
Router (config -if)#standby group-number ip virtual-ip-address
例如:     Interface  vlan10
          ip address  172.16.10.88  255.255.255.0
          no ip redirects                (关闭ICMP重定向)
          Standby 47 ip 172.16.10.11
```

❷ 配置该接口的 HSRP 备份优先级。

```
Router (config -if) Standby group-number priority priority-number
```

❸ 配置该接口的 HSRP 组中的备份优先权。

```
Router (config -if) standby group-number preempt
```

❹ 配置 HSRP 接口跟踪。在某些情况下，端口的状态直接影响着路由器的身份，即哪台路由器要变成活跃路由器，尤其是在每台路由器有到某个目的地的不同路径时。这是因为，当一个路由器的端口启用 HSRP 后，该端口将关闭 ICMP 重定向功能，因此，当有链路发生错误时，活跃路由器将不会对数据包进行重定向，导致数据包的人为不可到达。通过启用接口跟踪，可以根据接口的状态自动调整路由器的优先级，当被跟踪的端口变成不可用时，将自动降低其路由器的优先级，这样就降低了它继续成为活跃路由器的可能性。接口配置的模式下可作以下的配置。

```
Router(config-if)# standby group-number track type number interface-priority
```

其中，

type：跟踪的接口的类型，与接口号一起使用如 s0。

number：被跟踪的接口的号，与接口类型一起使用。

interface-priority:路由器要被降低的优先级的值，默认为 10。

例如，UTJS 大学的校园网边界路由器采用 HSRP 冗余的配置，其网络拓扑结构图如图 3-5 所示。

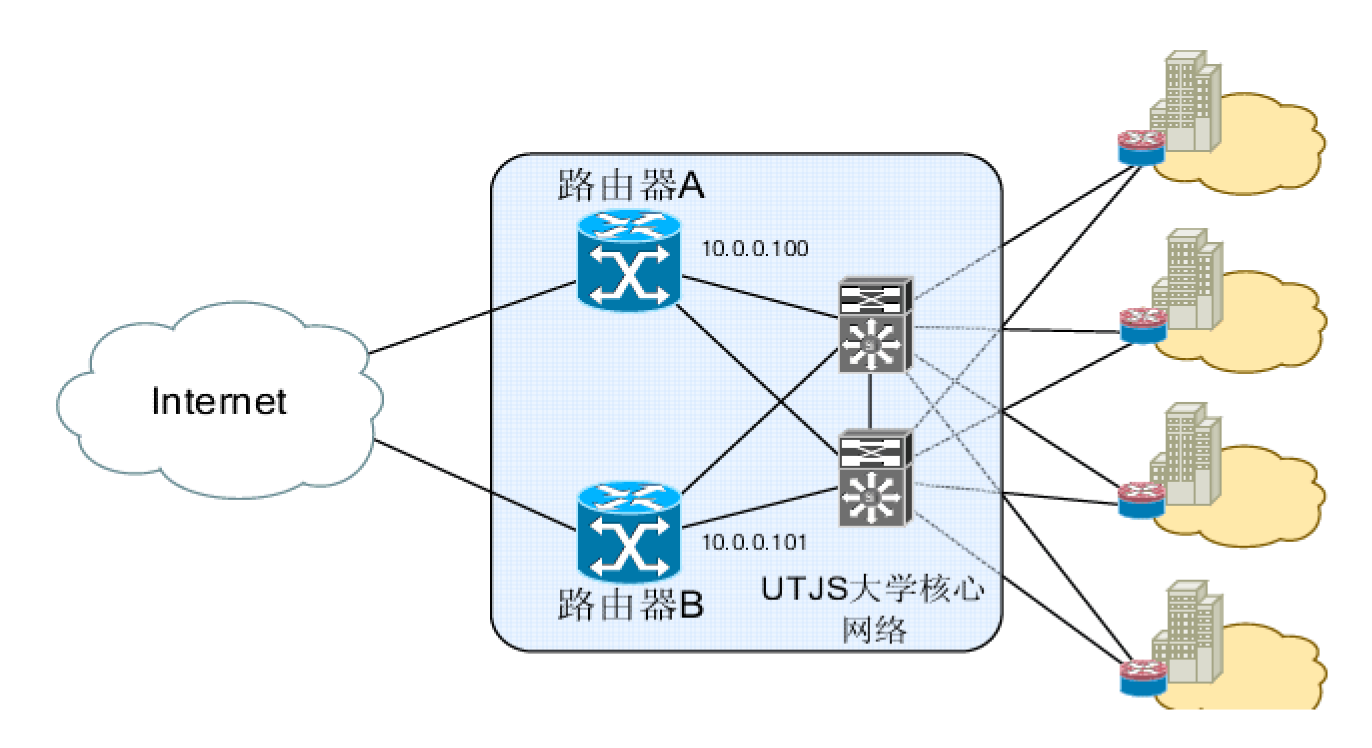


图 3-5 UTJS 大学边界路由器的 HSRP 冗余配置

在设计时，要求主要使用路由器 A，而将路由器 B 作为备份路由器，配置时可以使用热备份组优先级的方法。实际配置方式如下。

路由器 A：

```
interface Gi1/1
ip address 10.0.0.100
no ip redirects
stanby 1 ip 10.0.0.1
stanby priority 105
```

路由器 B：

```
interface Gi1/1
ip address 10.0.0.101
no ip redirects
stanby 1 ip 10.0.0.1
stanby priority 100
```

3.2.4 HSRP 安全

对于 HSRP，最大的问题是没有提供安全防护，在一个局域网内部，通过发送虚假的 UDP 多播数据包很容易对局域网中的路由器实施攻击，导致数据包黑洞(Packet Black Hole)和拒绝服务攻击(Denial-of-Service Attack)。一般是无法从一个局域网的外部实施攻击的，因为大多数路由器都不转发目的地址为所有路由器的多播地址(224.0.0.2)。

一般可以采用配置简单的认证和 MAC 绑定来增强 HSRP 的安全。下面分别介绍这两种方法。

1. HSRP 的认证功能

配置 HSRP 的认证功能的命令是：

```
Router(config-if)# standby group_number authentication string
```

2. 静态 MAC

通过给“热备份组”分配一个 MAC 地热，并与 IP 地址进行绑定，从而提高 HSRP 的安全，方法是：



```
Router(config-if)# standby group_number mac-address H.H.H.H
```

但是 MAC 地址可以更改，而认证消息本身就是明文，非常容易捕获。此时可以使用一种更安全的热备份协议 VRRP。

3.2.5　VRRP

虚拟路由器冗余协议(Virtual Router Redundancy Protocol，VRRP)可以把一台虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认网关。

在 VRRP 中，有两组重要的概念：VRRP 路由器与虚拟路由器，主控路由器与备份路由器。VRRP 路由器是指运行 VRRP 的路由器，是物理实体；虚拟路由器是指根据 VRRP 创建的路由器，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器。一个 VRRP 组中有且只有一台处于主控角色的路由器，可以有一个或者多个处于备份角色的路由器。VRRP 使用选择策略从路由器组中选出一台作为主控，负责 ARP 响应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当由于某种原因主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主控路由器。由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址，因此对于终端使用者系统是透明的。

一个 VRRP 路由器具有唯一的标识：VRID，范围为 0～255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。主控路由器负责对 ARP 请求用该 MAC 地址作应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 地址和 MAC 地址，减少了切换对终端设备的影响。

VRRP 控制报文只有一种：VRRP 通告。它使用 IP 多播数据包进行封装，组地址为 224.0.0.18，发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。为了减少网络带宽消耗，只有主控路由器才可以周期性地发送 VRRP 通告报文。备份路由器在连续三个通告间隔内收不到 VRRP 或收到优先级为 0 的通告后启动新的一轮 VRRP 选举。

在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 优先级范围是 0~255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器是 VRRP 组中的 IP 地址所有者。IP 地址所有者自动具有最高优先级 255，优先级 0 一般用在 IP 地址所有者主动放弃主控路由器角色时使用，用户可配置的优先级范围为 1~254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其他管理策略等。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由器的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。

为了保证 VRRP 的安全性，提供了两种安全认证措施：明文认证和 IP 头认证。明文认证方式要求在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。这种措施可以避免在局域网内的配置错误，但不能防止通过网络监听方式获得密码。IP 头认证的方式提供了更高的安全性，能够防止报文重放和修改等攻击。

对于图 3-5 所示的 UTJS 核心网络拓扑，采用 VRRP 配置的方式如下。

路由器 A：

```
interface Gi1/1
ip address 10.0.0.100
no ip redirects
vrrp 1 ip 10.0.0.1
vrrp 1 priority 100
vrrp 1 authentication md5 key-string d00b4r987654321a timeout 30
```

路由器 B：

```
interface Gi1/1
ip address 10.0.0.101
no ip redirects
vrrp 1 ip 10.0.0.1
vrrp 1 priority 200
vrrp 1 authentication md5 key-string d00b4r987654321a timeout 30
```

这样就可以实现相对安全的冗余协议了。同时，Cisco 路由器对于密码还支持 Key-Chain 的配置方式。这种方式类似于一个密码链，可以在一定的时候按照管理员的要求自动更改密码，从而可达到较高的安全性。

完成设备热备份协议的配置后，稍后的章节将介绍如何使用路由器冗余协议进行备份，以及路由器冗余协议的安全性配置等。

3.3 网络设备访问安全

应用实例导航：JS 公司远程访问漏洞修复

※场景呈现

2006 年 4 月 15 日，某人在 JS 公司到其分公司的链路上私自搭接了一台中继器，并使用 Wireshark 软件对流经该链路的数据进行侦听。某天当他查询侦听结果的时候，发现了一部分 Telnet 报文，如图 3-6 所示。

当他对数据流进行 TCP 复原的时候，让他“喜出望外”的事情发生了，这是某个网管员远程登录到一台路由器上进行配置的 Telnet 流量。他试着抓取了一部分登录的日志，如图 3-7 所示。

可以看到，在图 3-8 中的下半部分便是管理员输入的，将其编码方式调整为 Hex Dump，就可直接获取密码了，即“sjsj2611”为登录密码。不久，JS 公司的这台路由器即被攻破。

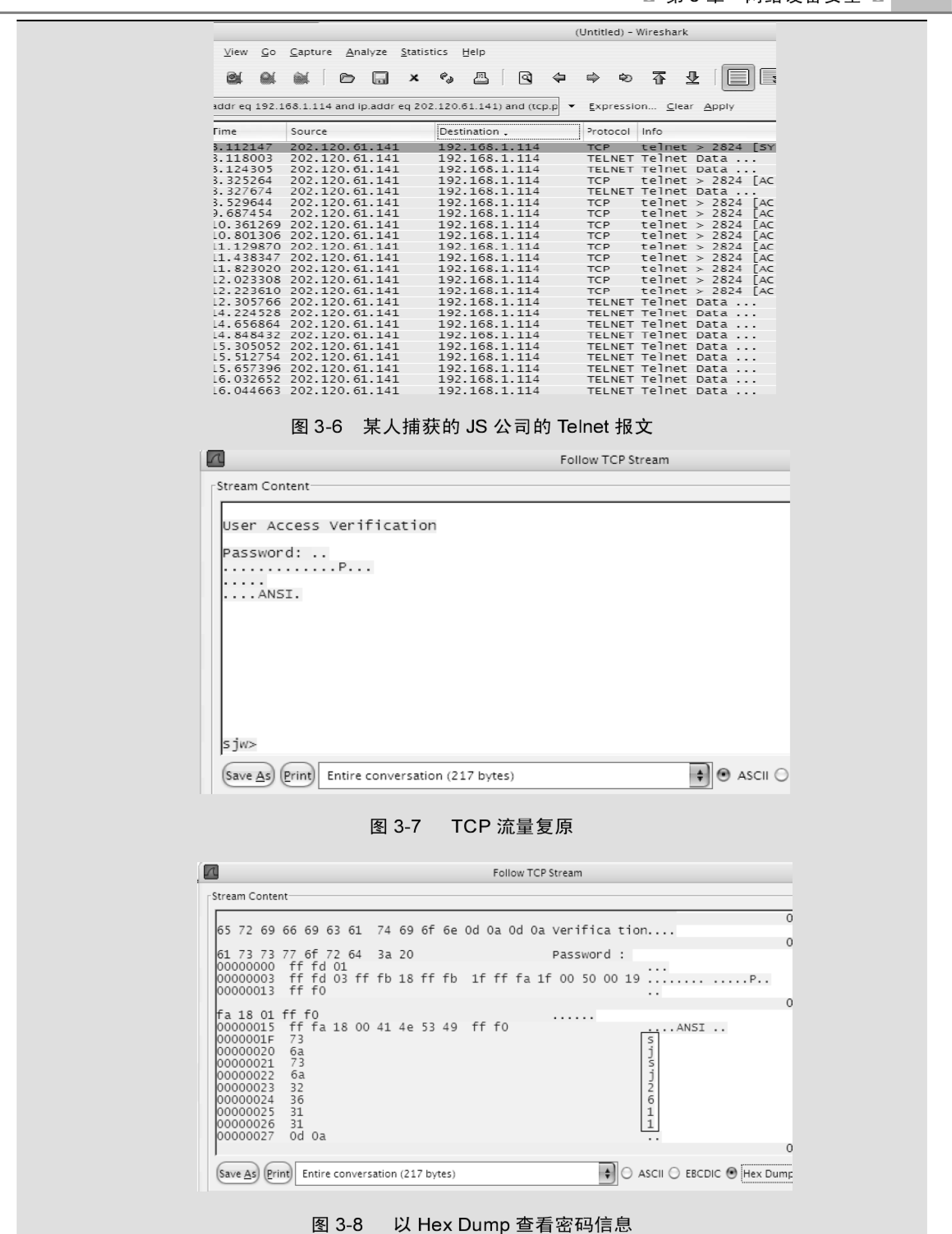


图 3-6　某人捕获的 JS 公司的 Telnet 报文

图 3-7　TCP 流量复原

图 3-8　以 Hex Dump 查看密码信息

※技术要领

(1) 网络设备安全登录的配置；
(2) 保存和查看网络设备产生的事件日志；
(3) SNMP 安全配置；
(4) 关闭网络设备中不必要的网络服务。

3.3.1 网络设备的安全登录

Telnet 已经是 Internet 上实现远程登录事实上的标准，网络管理员经常使用 Telnet 来远程维护交换机、路由器等网络设备。但由于 Telnet 的所有消息都是以明文进行传递的，这就给一些黑客造成可乘之机。为了保证远程维护网络设备时的安全，建议使用 SSP(Secure Shell，安全外壳)作为远程登录工具。SSH 是一种在不安全网络上提供安全远程登录及其他安全网络服务的协议，它在连接两端为主机和客户端时都使用认证密码，并且数据也经过加密后传输。

下面以 Cisco 路由器为例，说明 SSH 连接及其安全配置过程。

1 将用于远程登录的 vty 虚拟端口连接类型由 Telnet 转换为 SSH。

```
Router(config)#line vty 0 4
Router(config-line)#transport  input telnet ssh
```

2 限制能够远程登录的主机 IP 地址，并对非法地址进行日志记录。

```
Router(config)#access-list 1 permit host  10.16.58.1
Router(config)#Access-list 1 permit host  10.16.58.13
Router(config)#Access-list 1 permit host  10.16.8.1
Router(config)#Access-list 1 permit host  10.16.38.1
Router(config)#Access-list 1 deny any log
Router(config)#l Line vty 0 4
Router(config-line)# Access-class1 in
```

3 配置较短的超时时间以抵御 Telnet DDoS 攻击、劫持攻击等。例如，我们将超时时间设置为 3 分 30 秒，若在这段时间内没有数据流量，则断开连接。

```
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 3 30
```

4 为 vty 访问建立认证。用户认证可以采用本地认证和外置的 Radius 服务器认证两种方式，Radius 服务器认证方式将在第 7 章介绍，这里仅配置本地认证。

```
Aaa new-model
Aaa authentication login ciscojam local
Username cisco password ciscojam
Username ciscojam secret ccie

Line vty 0 4
Login authentication ccie
```

5 Router # show run 通过 show run 命令来查看运行中的配置文件。

```
hostname Router
```

```
!
…
username cisco password 0 ciscojam
username ciscojam secret 5 $1$L0DJ$qOYwof0dA5UHnsvZzXx/g/
```

❻ 上面所示的配置中，有一个名为 cisco 的账户密码是以明码形式存在的，需要开启加密服务，加密配置文件中的口令。

```
Router(config)#service password-encryption
```

❼ 查看运行中的配置文件，可以看到 cisco 账户的密码已经加密了。

```
Rount # show run
…
username cisco password 7 000A1A0B0B500A0D0E
username ciscojam secret 5 $1$L0DJ$qOYwof0dA5UHnsvZzXx/g/
…
```

3.3.2 保存网络设备日志

上文配置 SSH 登录检测日志时，可以将非法的 SSH 登录记录下来，以便网络管理员及时发现网络攻击。但在默认情况下，网络设备的日志都保存在本机上，当系统重启时日志便会丢失。更重要的是，这种方式也不便进行日志分析。因此，我们更希望网络设备产生的日志都能自动传送到一台服务器上，从而方便日志的存储或分析。

下面以 Cisco 路由器为例，说明网络设备日志配置过程。

❶ 设置日志缓冲区大小，一般该值为 16384。

```
Router(config)#Logging buffered 16384
```

❷ 设置 syslog 服务器 IP 地址，以便网络设备将日志发送给该服务器。

```
Router(config)#Logging 10.0.0.2
```

❸ 给日志加入时间戳。

```
Router(config)#Service  timestamps  log  datetime  [msec]  [localtime]
[show-timezone]
Router(config)#Service timestamps log uptime
```

❹ 如果需要可将日志发送到终端的 Telnet 会话中，以方便网管查看。

```
Router(config)#Terminal Monitor
```

❺ 配置日志消息类型。通常日志消息可分为如下几种类型。

```
Logging {console | monitor | trap | history} level
```

Level 分类如下。

0	Emergencies	系统不稳定
1	Alert	需要立即采取行动
2	Critical	临界情况
3	Errors	错误情况
4	Warnings	警告情况

5	Notifications	正常但重要的情况
6	Informational	仅信息消息
7	debugging	调试消息

❻ 如果要在本地查看或清除日志消息，可以使用如下命令。

```
Router#Show logging    //查看日志
Router#Clear logging   //清除日志
```

❼ 下面所示的是一个常见的路由器日志服务配置模板。

```
service timestamp debug datetime localtime show-timezone
service timestamp log datetime localtime show-timezone
clock timezone PST -8
clock summer-time PDT recurring
logging buffered 16384
logging trap debugging
logging facility local 7
logging 10.0.0.1
logging source-interface loopback 0
```

❽ 配置路由器后，还需要进一步配置接收这些日志的主机，通常为一台 Syslog 主机。Syslog 是一个运行在 UNIX 服务器上的进程或者守护进程，用于收集、储存日志文件，日志消息从运行在 UNIX 服务器上的不同服务以及其他网络结点发来，发送消息的服务指示其设备类型。Syslog 支持的设备类型如表 3-1 所示。

表 3-1　Syslog 支持的设备类型

设备类型	服　务
Auth	认证系统
Cron	时钟守护进程设备
Daemon	系统守护进程
Kern	内核
Local0-7	本地定义的消息
Lpr	打印系统
Mail	邮件系统
News	USENET 新闻
Sys9-14	系统使用
Syslog	系统日志
User	用户进程
Uucp	UNIX 到 UNIX 复制系统

❾ 修改/etc/sysconfig/syslog 文件，将其中的字段“SYSLOGD_OPTIONS="–m 0"”修改为“SYSLOGD_OPTIONS="–r –m 0"”

❿ Syslog 的配置文件是 /etc/syslog.conf，例如在该配置文件中加入如下命令。

```
Local7.debugging /usr/adm/logs/cisco.log
local7.notice    /usr/adm/logs/cisco.log
```

点评与拓展： 网络设备日志服务是网络设备最基本的配置，通过日志可以快速了解到大量的信息，并且将各种网络威胁阻止在发生的阶段。当然还有很多网络管理软件通过使用 SNMP 同样可以获取大量的信息。

3.3.3 SNMP 安全配置

SNMP(Simple Network Management Protocol，简单网络管理协议)为网络管理系统提供了底层网络管理的框架。SNMP 的应用范围非常广泛，诸多的网络设备、软件和系统中都有所采用，主要是因为 SNMP 有如下几个特点。

首先，相对于其他种类的网络管理体系或管理协议而言，SNMP 易于实现。SNMP 的管理协议、MIB 及其他相关的体系框架能够在各种不同类型的设备上运行，包括低档的个人电脑到高档的大型主机、服务器以及路由器、交换器等网络设备。一个 SNMP 管理代理组件在运行时不需要很大的内存空间，因此也就不需要太强的计算能力。SNMP 一般可以在目标系统中快速开发出来，所以它很容易在新产品或升级的老产品中出现。尽管 SNMP 缺少其他网络管理协议的某些优点，但它设计简单、扩展灵活、易于使用，这些特点大大弥补了 SNMP 应用中的不足之处。

其次，SNMP 是开放的免费产品。只有经过 IETF 的标准议程批准(IETF 是 IAB 下设的一个组织)，才可以改动 SNMP；厂商们也可以私下改动 SNMP，但这样做的结果很可能得不偿失，因为他们必须说服其他厂商和用户支持他们对 SNMP 的非标准改进，而这样做却有悖于他们的初衷。

再次，SNMP 有很多详细的文档资料(例如 RFC 以及其他的一些文档、说明书等)，网络业界对这个协议也有着较深入的理解，这些都是 SNMP 进一步发展和改进的基础。

最后，SNMP 可用于控制各种设备。比如电话系统、环境控制设备，以及其他可接入网络且需要控制的设备等，这些非传统设备都可以使用 SNMP。

正是由于上述特点，SNMP 已经被认为是网络设备厂商、应用软件开发者及终端用户的首选管理协议。

SNMP 是一种无连接协议，无连接是指它不支持如 Telnet 或 FTP 这种专门的连接。通过使用请求报文和返回响应的方式，SNMP 在管理代理设备和管理工作站之间传送信息。这种机制减轻了管理代理设备的负担，它不必非得支持其他协议及基于连接模式的处理过程。因此，SNMP 提供了一种独有的机制来处理可靠性和故障检测方面的问题。

另外，网络管理系统通常安装在一个比较大的网络环境中，其中包括大量的不同种类的网络和网络设备。因此，为了划分管理职责，应该把整个网络分成若干个用户团体(Community)，将满足一定条件的网络设备归为同一个 SNMP 团体。SNMP 支持这种基于团体字符串(Community String)信息的安全模型，可以通过物理方式把它添加到选定的团体内的每个网络设备上。

目前，SNMP 中基于团体字符串的身份验证模型被认为是很不牢靠的，存在一个严重的安全问题。主要原因是 SNMP 并不提供加密功能，也不保证在 SNMP 数据包交换过程中不从网络中直接传递团体字符串信息。只需使用一个数据包捕获工具就可把整个 SNMP 数据包解密，这样团体字符串就暴露无遗了。正是因为这个原因，大多数站点禁止管理代理设备的设置操作。但这样做有一个副作用，这样一来只能监控数据对象的值而不能改动它们，限制了 SNMP 的可用性。

SNMP 在版本 1 和版本 2 中由于使用团体字符串，将会带来很多安全性问题，仅在版

本 3 中，才支持 MD5/SHA 的认证方式，对于消息也仅有 C3 支持 DES 加密。表 3-2 所示为 SNMP 的版本。

表 3-2　SNMP 的版本

版　本	级　别	认　证	加密	注　释
版本 1	NoAuthNoPriv	团体字符串	无	利用团体字符串匹配进行认证
版本 2	NoAuthNoPriv	团体字符串	无	利用团体字符串匹配进行认证
版本 3	NoAuthNoPriv	用户名	无	利用用户名匹配进行认证
版本 3	AuthNoPriv	MD5/SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 认证算法
版本 3	AuthPriv	MD5/SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 认证算法。除提供 CBC-DES(DES-56)标准进行认证外还提供 DES-56 位的报文加密

下面简要介绍在 Cisco ISO 路由器或交换机中开启 SNMP 服务的配置方法，其他厂家生产的网络设备的配置方法与之类似。

❶ 进入特权配置模式，使用 snmp-server community 命令创建只读和可读写团体字符串。

```
Router#config terminial
Router(config)#snmp-server community <只读团体字符串> ro
Router(config)#snmp-server community <可读写团体字符串> rw
```

❷ 配置 SNMP 引擎，这是一个可选配置。

```
Router(config)#snmp-server engineID [local engineid-string] | [remote
ip-address udp-port port engineid-string]
```

❸ 配置 Trap 服务类型。

```
Router(config)#snmp-server host host-addr [traps | informs] [version {1 |
2c | 3 [auth | noauth | priv]}]      //其中auth为SHA和MD5， priv 为DES
Router(config)#community-string [udp-port port] [notification-type]
```

❹ 配置 Trap 消息类型。

```
Router(config)#snmp-server enable traps [notification-type] [notification-option]
```

❺ 如果要使用 SNMP 消息 reload 路由器，则需要输入如下命令。

```
Router(config)#snmp-server system-shutdown
```

❻ 如果要使用 TFTP 服务器来存取配置文件，可以用访问控制列表限制 TFTP 的访问。

```
Router(config)#snmp-server tftp-server-list acl-number
```

❼ 下面是一个配置实例，要求 172.16.1.200 和 201 以只读方式接收 bgp 陷阱消息。

```
snmp-server community access RO
snmp-server enable traps bgp
snmp-server host 172.16.1.200 access
snmp-server host 172.16.1.201 access
```

❽ 可以通过下面的方法来验证配置。

```
Router#clear ip bgp *
SNMP: Queuing packet to 172.16.1.200
SNMP: V1 Trap, ent bgp, addr 10.1.2.25
 bgpPeerEntry.14.10.1.2.1 = 00 00
 bgpPeerEntry.2.10.1.2.1 = 1
SNMP: Queuing packet to 172.16.1.201
SNMP: V1 Trap, ent bgp, addr 10.1.2.25
 bgpPeerEntry.14.10.1.2.1 = 00 00
 bgpPeerEntry.2.10.1.2.1 = 1
SNMP: Packet sent via UDP to 172.16.1.200
SNMP: Packet sent via UDP to 172.16.1.201
```

点评与拓展：SNMP 是最常用的网络管理协议，它能系统详细地读取设备的数据库，并获取设备的工作状态，例如接口流量等。通常这样的数据库称作 MIB 数据库。MIB 数据库为一种树形结构，各值所代表的不同意义可以在设备厂商所提供的资料中查询，用于完成一些自定义的检测和响应任务。

3.3.4　禁用不必要的服务

在很多路由器中都启用了很多网络服务以支持第二、三、四、七层的网络协议。以 Cisco 路由器为例，管理员可以开启 BOOTP 协议，使得其他路由器能够在启动时进行 IOS 复制；开启 CDP 协议，可以查找其他邻居的 Cisco 设备；开启 NTP 服务，以提供网络时间同步功能，等等。为了保证路由器和交换机的安全，可以将这些服务关闭。

✧ 关闭 Finger 服务。Finger 服务用于 UNIX 用户查找服务(lookup)，允许用户远程访问。如果不需要该功能，可以使用如下命令来关闭 Finger 服务。

```
Router(config)#no ip finger
Router(config)#no service finger
```

✧ 关闭 HTTP 服务。HTTP 服务用于支持一些 Cisco 设备的 Web 配置，如果不需要该功能，可以使用如下命令来关闭 HTTP 服务。

```
Router(config)#no ip http server
```

✧ 关闭 BOOTP 服务。BOOTP 服务用于某些 Cisco 路由器使用 BOOTP 协议通过网络来获取 IOS，然后启动。如果 Cisco 路由器直接从 Flash 中获取 IOS，可以将该服务关闭。

```
Router(config)#no ip boot server
```

✧ 关闭 CDP 服务。CDP 服务用于发现与之直接相连的 Cisco 邻居设备，以便排除网络故障。如果不需要该服务，可以将其关闭。

```
Router(config)#no cdp run
```

下面是一个禁用不需要服务的边界路由器配置模板。

```
Router(config)#no ip source-route
Router(config)#no ip classless
```

```
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
Router(config)#no ip finger
Router(config)#no service finger
Router(config)#no ip bootp server
Router(config)#no ip http server
Router(config)#no ip name-server
Router(config)#no boot network
Router(config)#no service config
Router(config)#no snmp-server
```

除了上述在全局停止一些网络服务外，还可在接口上拒绝接收一些容易受到攻击的服务的报文。方法如下。

```
Router(config)#interface Ethernet0
Router(config-if)# ip address dhcp
Router(config-if)# no ip redirects
Router(config-if)# no ip unreachables
Router(config-if)# no ip proxy-arp
Router(config-if)# ntp disable
```

交换机及路由器中的很多服务都是使用面向非连接的 UDP。为了安全起见，可以将这些服务报文的源地址设置为回环接口。方法如下。

```
Router(config)# snmp-server trap-source loopback 9
Router(config)#ip tftp source-interface loopback 9
Router(config)#ip radius source-interface loopback 9
Router(config)#ip telnet source-interface loopback 9
Router(config)#logging source-interface loopback 9
```

3.3.5 登录警告

一些安全区域内的设备，如果登录时发生警告，则对于闯入系统的黑客进行相应的民事或者刑事起诉将会十分容易。通常警告的配置方式如下。

```
Router(config)#banner {exec | incoming | login | motd }  message
```

下面是一个登录警告的例子。

```
Router(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Warning : You are connected a monitored network.
Unauthorized access and use of this network will be vigorously prosecuted
---===nxxx.com===---
#
```

3.4 本 章 小 结

本章我们介绍了如何设计一个可靠的网络，针对一些比较容易发生的漏洞做了攻击演示，并对这些漏洞进行了修补。简要介绍了 Wireshark 等抓包分析软件，介绍了 Cisco 的 SDM 安全配置管理器，通过它可以实现基于 Web 的安全访问控制。

第 4 章　路由器及路由协议安全

路由器是网络中最常见的网络设备，由于通常负责大量的数据转发，因此它常常成为众多黑客的有效攻击对象。路由器安全是局域网网络安全中的一个重要话题，本章我们将学习如何使路由器变得更加安全。

通过本章的学习，读者应掌握以下主要内容：

✧ 路由协议安全
✧ 访问控制
✧ 路径完整性检查
✧ 黑洞过滤

4.1　路由协议安全概述

在一个安全的网络中，其中的流量怎样流动是网络安全的最根本问题，控制流量流动方向的是路由协议，所以需要确保路由协议与网络安全的需求相一致。毋庸置疑，一个有安全的路由体系结构的网络与一个路由结构设计有缺陷的网络相比，前者更不容易受到攻击，而后者可能会受到致命性的攻击。

1. 路由过滤

适当的路由过滤对于网络安全是非常重要的，在一个有路由连接到外部 Internet 的专用网络中尤其重要。在这些网络中，必须确保路由过滤用于过滤出那些进入专用网络的路由和不受欢迎的路由，并确保只有真正包含在内部网络上的路由才能允许通告。

路由过滤的作用是使得真正需要对外访问的用户能够访问到网络，而隔断内部涉及机密的数据服务器对外的连接。通常，一些私有地址是禁止通告到互联网上的，这些地址如下。

✧ 0.0.0.0/0：用于默认路由。
✧ 127.0.0.0/8：主机回环地址。
✧ 10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16：RFC1918 定义的专用地址。
✧ 169.254.0.0/16：Windows 等系统终端结点自动配置的 DHCP 地址段。
✧ 192.0.2.0/24：测试地址段，用于供应商文档示例。
✧ 224.0.0.0/3：组播地址段。

除了上述这些专用地址，还有一些专用网络的 IP 地址段也不允许流出到外部的网络上。这是一个必要的防范措施，它能保护一些在内部网络上的主机流量不会被无意地通告到外部路由器上。

在一个局域网络中，通常我们会将其划分为不同的区域，每个区域有特定的安全等级。从低安全等级区域访问到高安全等级的区域通常我们可以配备适当的防火墙和其他认证机制，然后通过路由过滤的方式将流量引入通过防火墙的链路。另外，我们也可以人为地隔断从低安全网络区域到达高安全网络区域的能力。

正确地应用路由过滤，还可以将地址段汇总，对外隐藏自己的网络拓扑，并且在内部网络部分区域出现故障后，设置在边界路由器上的出口过滤能够阻止故障在网络上蔓延。

对于运营商而言，它们可以使用策略路由过滤的方式。通常为了保证 Internet 上的 BGP 转发路由条目较少，运营商要求地址前缀大于 20 的路由不能通告到运营商网络，而这样的策略就是使用策略路由过滤器实现的。

2. 恰当地使用静态路由

在大多数情况下，动态路由协议给网络的稳定性和灵活性提供了很好的平台。但是很多时候还是需要用到静态路由，并且静态路由常用于默认路由的通告和一些具有明显特征的流量控制。由于其管理距离优先级高于动态路由，通常还可以在网络遭受攻击时，通过它来阻断攻击者和网络的链接，过滤攻击流量。

3. 网络收敛速度

快速收敛对于一个安全的网络是非常重要的，在网络受到破坏进行回复的时候， 收敛慢的网络可能需要较长的时间，这将会使问题进一步恶化。在 Internet 范围内，对于大型网络而言，特别是运营商网络，它们所使用的 BGP 域间路由，如果收敛慢将会意味着相当客观的收入大量损失。即便是对一个相对较小的园区网络而言，也意味着较大的生产力受到破坏。

慢收敛的网络通常还会遇到一个问题：更加容易遭受拒绝服务(DoS)攻击。通常 DoS 攻击可以是一个或者两个结点出现故障， 如果此时网络需要花费大量的时间用于收敛，将意味着 DoS 攻击实际上只攻击一个结点就会导致大量的结点失效了。

收敛性通常依赖于很多不同的因素，包括网络体系结构的复杂性、网络区域划分、网络冗余是否存在、不同路由器路由计算设置的参数等。对于网络管理员而言，有责任去提高网络的收敛速度，并且根据加快收敛性的策略来设计网络，提高收敛速度。

4.2 增强路由协议的安全

路由协议运行时，通常信任端路由器发来的任何消息且不作验证，这样就导致了一些特殊的攻击行为。例如，某些路由协议采用组播的方式发送路由消息，这样监听者就可以采用相同的方式伪造组播报文，导致受攻击的路由器不仅受骗将数据发送到不正确的地址，而且灵活的操纵策略也完全不能运作。有时还能简单地诱导路由改变，以将流量重定向到网络中适当的位置以便攻击者分析，这样导致了攻击者能够区分流量模式并获得并不是发给他的消息。

4.2.1　路由协议的认证方法

促进路由协议认证的原因来自大量的黑客攻击行为从应用层逐渐下移，并且随着 BGP 路由协议的提出大量应用于 Internet，运营商将更加担心这样的核心路由器被一个假冒的 BGP 邻居控制，而一个 BGP 路由器通常会通告大量的路由信息，当一台路由器遭受攻击时大量的业务将被影响。

通常大部分路由协议在进行消息交换时，通过携带特定的消息字段来进行验证，如图 4-1 所示。

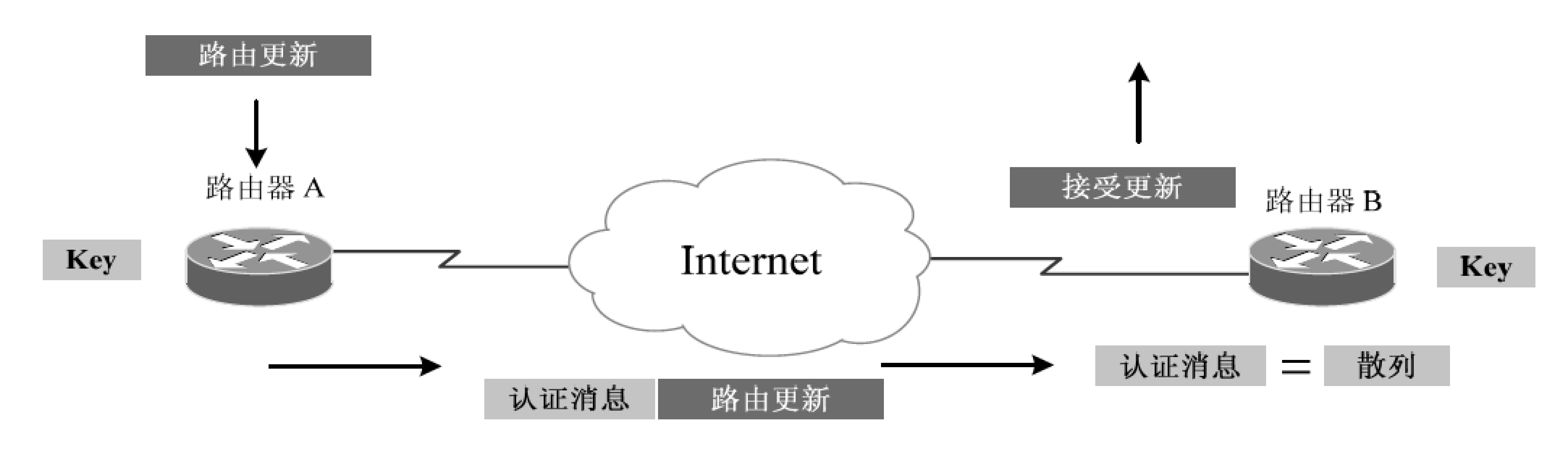


图 4-1　路由协议认证原理

通常对于认证消息字段可以使用明文密码和 MD5-HMAC 两种方式进行处理。

1. 明文加密

通过使用一个明文字符串(Key)，随着路由更新消息一同发送到另一个路由器上，另一个路由器上如果设置了同样的字符串，则该路由消息会验证成功，从而接受路由更新消息。但是这并不是一个很安全的加密方式，稍微熟练的一个黑客就能轻松截取到 A 发送到 B 的消息，并使用这样的一个纯字符串伪造消息。

2. MD5-HMAC 加密

MD5-HMAC 算法就是为了避免密钥以明文形式在网络中传播，它使用配置的密钥进行一个加密的散列算法计算。首先发送端路由器 A 将路由更新消息作为输入文本，利用密钥和散列函数进行计算得到一个散列值。接着，将这个散列值随着路由更新消息一同传输给接收端路由器 B。接收端的路由器 B 将接受到的路由更新消息作为文本，并把自己的密钥放入散列函数，计算出一个新的散列值，与路由器 A 传来的散列进行比较，如果相同则接受消息。

值得我们关注的是，第二种算法一方面解决了路由器相互之间加密认证的问题，另一方面也对收到的消息做了完整性检验。一旦某个攻击者截获了路由信息，由于没有密钥，即便是使用相同的散列，作为文本输入的路由更新消息也会随着改变，将导致验证失败。

4.2.2　RIP 协议安全

应用实例导航：UT 大学路由协议攻击与防范

※场景呈现

小 A 是 UT 大学计算机系的一名学生，在某次做计算机网络大作业的时候，使用 Wireshark 截获了如图 4-2 所示的报文。

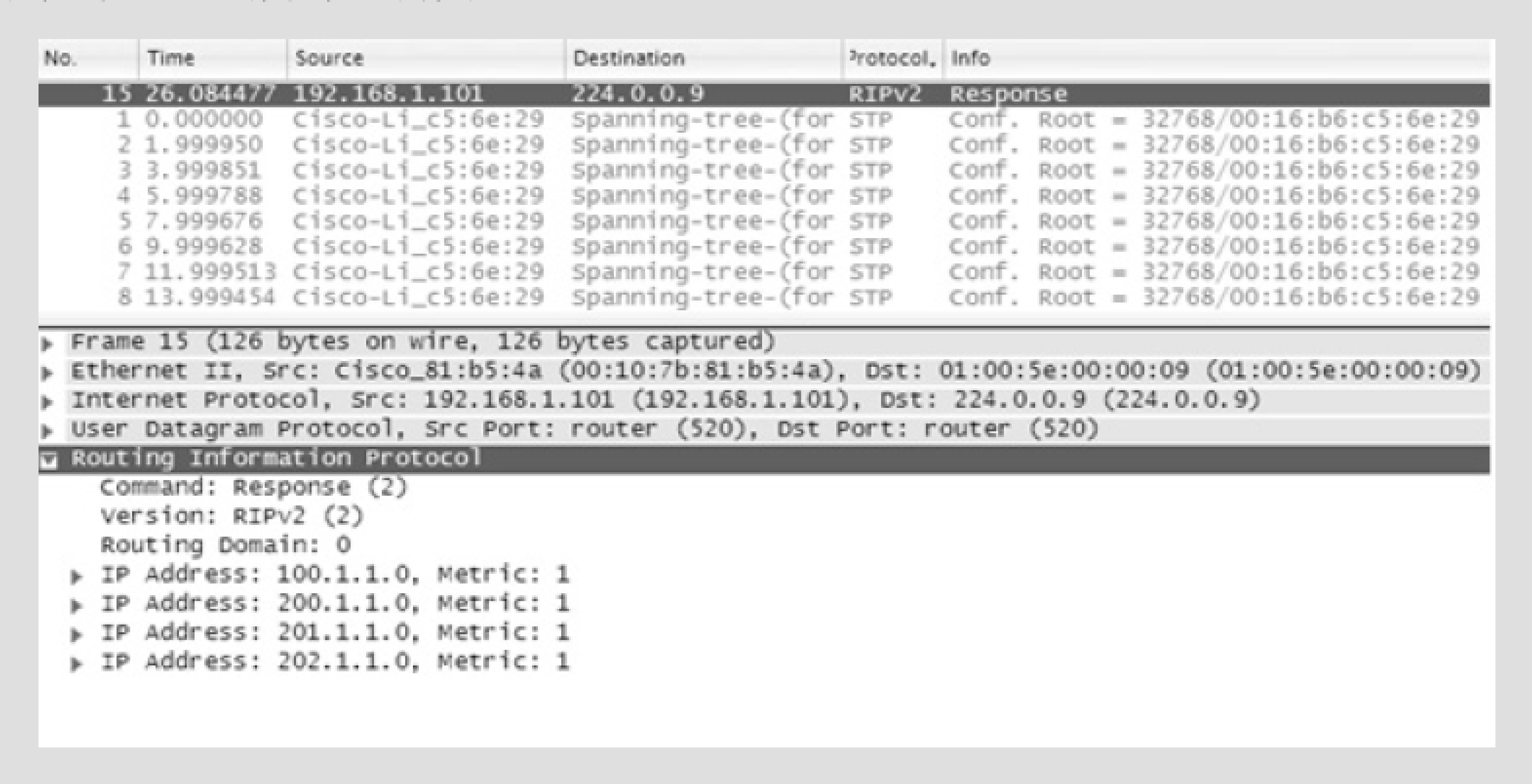


图 4-2　小 A 截获的 RIP 信息报文

从图 4-2 可以看出，小 A 所在的网络接口上路由器的 RIP 路由协议没有关闭，并且可以看到对方路由器的 IP 地址为 192.168.1.101，通告的地址段为 100.1.1.0、200.1.1.0、201.1.1.0 和 202.1.1.0。此后小 A 通过伪造 RIP 路由协议信息报文将大量的路由信息注入到接入路由设备中，使学校部分网络瘫痪。

如果小 A 将更多的地址(例如 100 万条路由条目)注入，校内路由设备将会不堪重负，不停地死机重启，从而产生更大规模的网络中断。

图 4-3 所示为 UT 大学网络拓扑，小 A 攻击的就是 A 校区的路由器 Router A。

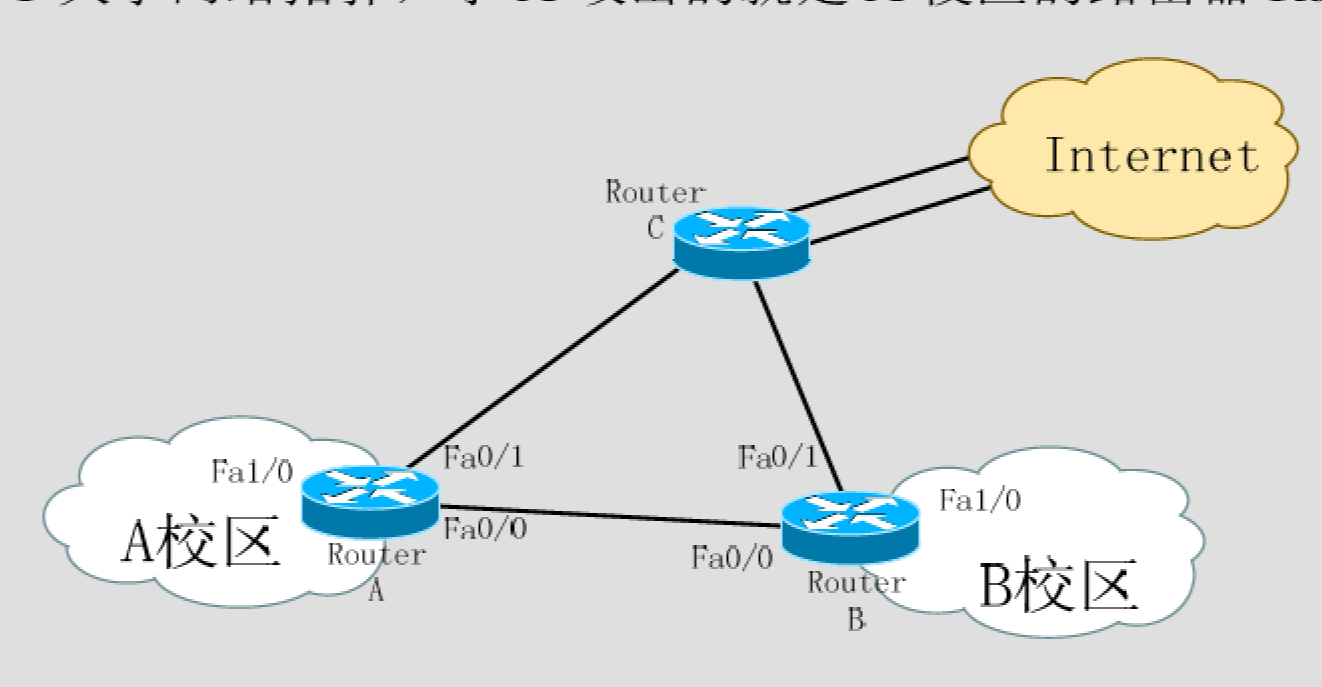


图 4-3　UT 大学网络拓扑



※技术要领

(1)　配置 RIP 报文认证；
(2)　关闭 RIP 的路由更新。

路由信息协议(Routing Information Protocol，RIP)是以跳数作为度量值(Metric)的距离向量协议。RIP 广泛用于全球因特网的路由，是一种内部网关协议(Interior Gateway Protocol，IGP)，即在自治系统内部执行路由功能。

1. 配置 RIP 报文认证

RIP 协议有两种版本：第一版(RIPv1)和第二版(RIPv2)。RIPv1 没有使用认证机制并使用不可靠的 UDP 协议进行传输，天生就有不安全因素。RIPv2 的分组格式中包含了一个选项，可以设置 16 个字符的明文密码字符串(表示可以很容易地被嗅探到)或者 MD5 认证。虽然 RIP 信息包可以很容易伪造，但在 RIPv2 中使用 MD5 认证将会使欺骗的操作难度大大提高。

下面简要地介绍一下配置 RIP 报文认证的过程。

❶ 在路由器上指定密钥链(Key chain)的名字。

```
Router(config)#key chain jam
```

❷ 定义一个密钥，并设定这个密钥。

```
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string mike
```

❸ 进入需要认证的接口，并配置 RIP 认证信息。

```
Router(config)#int s0 (进入需要认证的接口)
Router(config-if)#ip rip authentication key-chain jam (使用密钥链)
```

❹ 默认情况下，加密方式使用明文方式；若要使用 MD5 认证，可以执行如下命令。

```
Router(config-if)#ip rip authentication mode md5
```

❺ 配置后使用 debug ip rip events 命令，可以看到当密钥不匹配时会出现如下消息。

```
Router#debugip rip events
*Mar  1 03:26:46.016: RIP: ignored v2 packet from 1.1.1.2 (invalid
authentication)
```

❻ 为了密码安全我们还可以在一个密钥链中定义多个密钥，并按一定的时间顺序进行修改。

```
  key chain jam
      key 1
        key-string mike
        accept-lifetime 16:30:00 Nov 28 2004 duration 43200 (持续43200秒)
        send-lifetime 16:30:00 Nov 28 2004 duration 43200
      key 2
        key-string love
        accept-lifetime 04:00:00 Nov 29 2004 13:00:00 Apr 15 2005(到期时间)
        send-lifetime 04:00:00 Nov 29 2004 13:00:00 Apr 15 2005
      key 3
        key-string baby
        accept-lifetime 12:30:00 Apr 15 2005 infinite (永远)
```

```
send-lifetime 12:30:00 Apr 15 2005 infinite
```

❼ 重复上述步骤，配置其他参与 RIP 路由协议的路由器。

2. 关闭路由更新

使用密钥可以非常容易提高路由器的安全性，但是 RIP 路由协议可以接受来自任何设备的路由更新，因此上述方法并不是一劳永逸的办法。为了解决上述问题，我们可以将一些不需要接收和转发路由信息的端口设置为被动端口(Passive interface)。

❶ 将不需要转发路由信息的端口设置为被动端口。

```
Jam(config)#router rip
Jam(config-router)#passive-interface Ethernet0
```

❷ 将端口设置为被动端口后，需要指定路由更新邻居，否则路由器之间将无法接收到路由更新。

```
Jam(config-router)#neighbor 172.17.1.2
```

3. 配置实例

在上述“应用实例导航”中，小 A 攻击的是 Router A，连接端口是 Fa1/0 接口，因此我们需要将这个接口的路由更新信息关闭；和其他路由器相连时，采用限定邻居的单播方式相连，并根据不同的时间使用不同的密钥，加密类型为了网络安全采用 MD5。下面是为 UT 大学网络配置安全的 RIP 协议的过程。

❶ 将 Router A 和 Router B 的相应端口设置为被动端口。

```
RouterA(config)#router rip
RouterA(config-router)#version 2   //一定要开启版本2模式才能获得加密认证功能
RouterA(config-router)#passive-interface FastEthernet 1/0
RouterA(config-router)#passive-interface FastEthernet 0/0
RouterA(config-router)#passive-interface FastEthernet 0/1
RouterB(config)#router rip
RouterB(config-router)#version 2
RouterB(config-router)#passive-interface FastEthernet 1/0
RouterB(config-router)#passive-interface FastEthernet 0/0
RouterB(config-router)#passive-interface FastEthernet 0/1
```

❷ 将路由器 A 和 B 设置为邻居关系。

```
RouterA(config-router)#neighbor 172.17.1.1   // Router B  Fa0/0接口的IP地址
RouterB(config-router)#neighbor 172.17.1.2   // Router A  Fa0/0接口的IP地址
```

❸ 根据时间配置密钥链。

```
RouterA(config)#key chain RouterA
RouterA(config-keychain)#key 1
RouterA(config-keychain-key)#key-string cisco
RouterA(config-keychain-key)#accept-lifetime 16:30:00 Nov 28 2004 duration
43200
RouterA(config-keychain-key)#send-lifetime 16:30:00 Nov 28 2004 duration
43200
RouterA(config-keychain-key)#key 2
RouterA(config-keychain-key)#key-string love
RouterA(config-keychain-key)# accept-lifetime 04:00:00 Nov 29 2004 13:00:00
Apr 15 2005
RouterA(config-keychain-key)# send-lifetime  04:00:00 Nov 29 2004 13:00:00
Apr 15 2005
```

```
RouterA(config-keychain-key)#key 3
RouterA(config-keychain-key)#key-string yourcisco
RouterA(config-keychain-key)#accept-lifetime 12:30:00 Apr 15 2005 infinite
RouterA(config-keychain-key)#send-lifetime 12:30:00 Apr 15 2005 infinite

RouterB(config)#key chain RouterB
RouterB(config-keychain)#key 1
RouterB(config-keychain-key)#key-string cisco
RouterB(config-keychain-key)#accept-lifetime 16:30:00 Nov 28 2004 duration
43200
RouterB(config-keychain-key)#send-lifetime 16:30:00 Nov 28 2004 duration
43200
RouterB(config-keychain-key)#key 2
RouterB(config-keychain-key)#key-string love
RouterB(config-keychain-key)# accept-lifetime 04:00:00 Nov 29 2004 13:00:00
Apr 15 2005
RouterB(config-keychain-key)# send-lifetime  04:00:00 Nov 29 2004 13:00:00
Apr 15 2005
RouterB(config-keychain-key)#key 3
RouterB(config-keychain-key)#key-string yourcisco
RouterB(config-keychain-key)#accept-lifetime 12:30:00 Apr 15 2005 infinite
RouterB(config-keychain-key)#send-lifetime 12:30:00 Apr 15 2005 infinite
```

❹ 将密钥链应用到需要进行认证的网络接口上。

```
RouterA(config)#int FastEthernet 0/0
RouterA(config-if)#ip rip authentication key-chain RouterA
RouterA(config)#int FastEthernet 0/1
RouterA(config-if)#ip rip authentication key-chain RouterA
RouterB(config)#int FastEthernet 0/0
RouterB(config-if)#ip rip authentication key-chain RouterB
RouterB(config)#int FastEthernet 0/1
RouterB(config-if)#ip rip authentication key-chain RouterB
```

❺ 定义加密方式为明文或者 MD5 加密，这里使用 MD5 加密。

```
RouterA(config-if)#ip rip authentication mode md5
RouterB(config-if)#ip rip authentication mode md5
```

点评与拓展：对于 UT 大学，采用 RIP 路由协议安全的配置以后，小 A 通过抓包工具将再也无法看到有关 RIP 协议的消息了， UT 大学网络安全性提高了。但是 RIP 路由协议由于最大跳数为 16，因此不可能用于大规模网络，同时由于其路由更新机制，收敛速度相对于 OSPF 等路由协议慢很多，所以对于大型网络，我们将在下一节介绍 OSPF 协议安全。

4.2.3　OSPF 协议安全

应用实例导航：UT 大学网络配置安全的 OSPF 协议

※场景呈现

图 4-4 为前文所述的 UT 大学网络拓扑结构图，随着学校的发展，网络规模扩大，现在

该校网路上的路由协议为 OSPF，小 A 攻击的区域仍然是 A 校区的路由器 Router A。

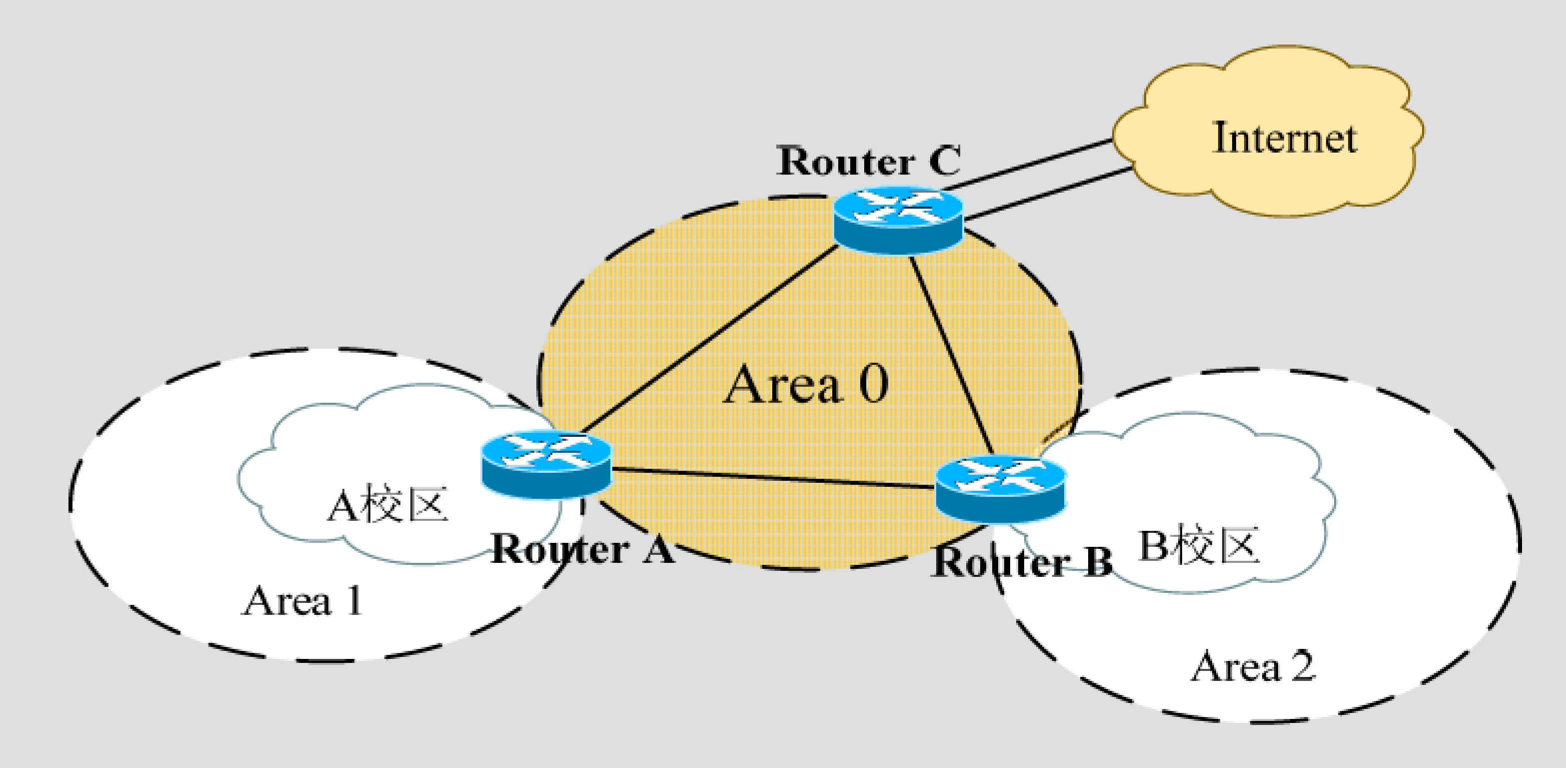


图 4-4 UT 大学网络拓扑结构图

※技术要领

(1) 配置 OSPF 非广播邻居；
(2) 配置 OSPF 路由器认证；
(3) 禁用不需要 OSPF 路由协议接口的 OSPF 更新；
(4) 配置端区；
(5) 配置路由器 ID；
(6) 配置 SPF 计时器；
(7) 配置 OSPF 路由过滤。

OSPF(Open Shortest Path First，开放式最短路径优先)路由协议是一个用于在单一自治系统(Autonomous system，AS)内的决策路由，它是最常用的 IGP 路由协议之一。与 RIP 不同，OSPF 是链路状态路由协议，而 RIP 是距离向量路由协议。同时，OSPF 路由协议可以将网络划分为不同的区域，并且可以采用多种区域属性和认证方式，安全性和灵活性相对于 RIP 高了很多，并且路由收敛速度更快。

1. 配置 OSPF 非广播邻居

OSPF 路由器与邻居通信时，很多情况下是使用组播方式，为了防止受到假冒路由器的攻击，因此需要将一些链路的通信方式修改为单播方式。

❶ 将路由器配置为单播更新路由信息。

```
Router(config)#ip ospf network point-to-multipoint non-boardcast
```

❷ 在路由器的 OSPF 进程中配置邻居。

```
Router(config)#router ospf 1
Router(config-router)#neighbor 172.1.1.1
Router(config-router)#neighbor 172.1.1.2
Router(config-router)#neighbor 172.1.1.3
```

2. 配置 OSPF 路由器认证

OSPF 邻居路由器认证通过路由器上接收到的任何 OSPF 源进行。来自一个 OSPF 源的

消息如果不被认证，将会被丢弃。

OSPF 认证消息比较灵活，由于 OSPF 有区域的概念，所以相对于 RIP 路由协议而言，OSPF 既可以在接口上进行消息认证，也可以对某个区域进行认证。

❶ 在路由器参与 OSPF 路由交换的接口上配置认证。

```
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip ospf message-digest-key md5 cisco
```

❷ 在路由器的 OSPF 进程中配置区域认证。

```
Router(config)#router ospf 1
Router(config-router)#area 0 authentication message-digest
Router(config-router)#area 1 authentication message-digest
```

3. 禁用不用的接口

除了认证外，对于不需要 OSPF 路由协议的接口，可以通过配置把这些接口的 OSPF 更新能力关闭，即将某一接口配置为被动接口。

```
Router(config)# router ospf 100
Router(config-router)# passive-interface FastEthernet 1/3
```

4. 配置端区

OSPF 是一个可以把网络划分成不同区域的路由协议，整个网络的中心区域号必须为 0，我们将这个区域称为骨干区域(Backbone area)。通常其他非 0 区域只能连接到 0 区域才能通信，如图 4-5 所示。

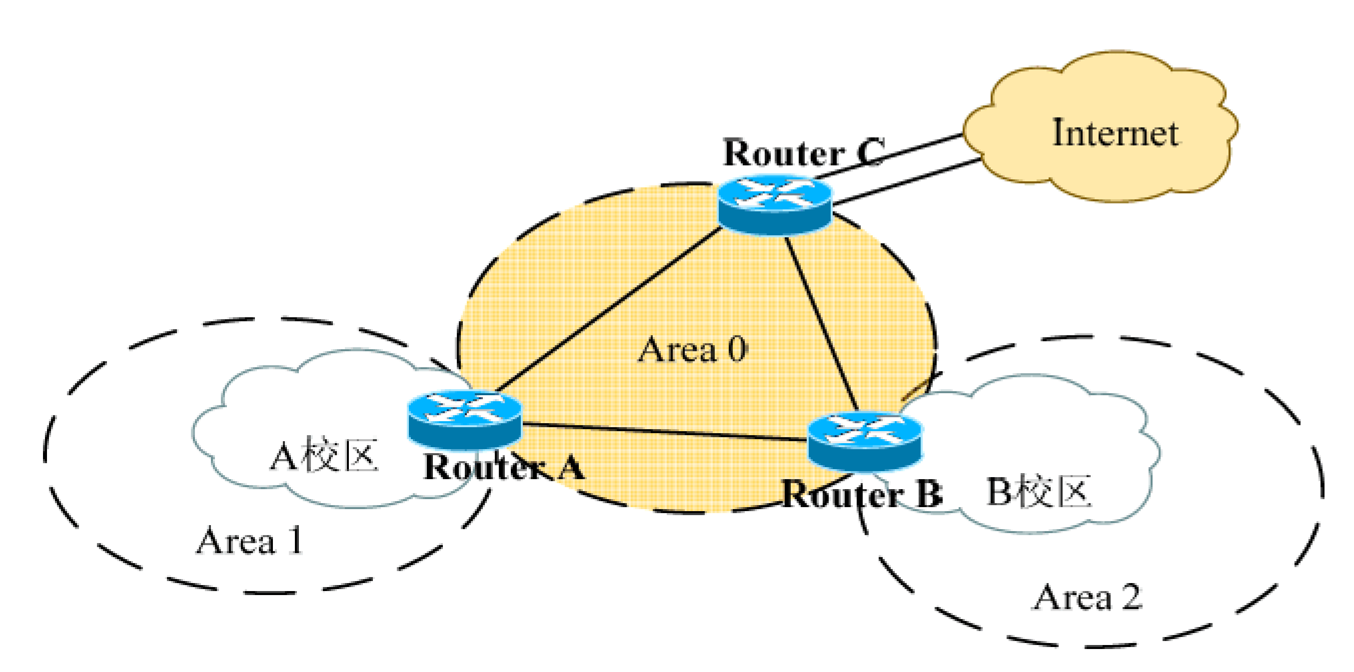


图 4-5　OSPF 区域

在区域属性中，定义了一种端区(Stub area)属性，它能够使外部路由中的信息不能被发送进入到该区域中，并且在端区内的路由器依赖于区域边界路由器(ABR，如图 4-5 中的 Router A 和 Router B)产生一个默认路由发送目的地为端区外的数据包。使用端区对安全有利，因为整个区域被迫只有一个单一的通过 ABR 的出口，这样网络管理员可以通过监视恶意活动了解这个单一出口。端区的另一个优点是降低了路由器的负载，因为端区内的路由器仅能和一条来自 ABR 的默认路由一起工作，而不是其他区域的所有路由，这种降低负载的行为从某种意义上说是提高了稳定性，特别是在网络受到攻击的时候，网络稳定性和安全性具有相同的含义。

端区的配置方式如下。

❶ 将 ABR 路由器上配置端区。

```
RouterB(config)# router ospf 100
RouterB(config-router)# area 2 stub no-summary
RouterB(config-router)# area 2 default cost 10
```

❷ 配置端区内其他所有路由器。

```
RouterB1(config)# router ospf 100
RouterB1(config-router)# area 2 stub
RouterB2(config)# router ospf 100
RouterB2(config-router)# area 2 stub
```

5. 配置路由器 ID

在默认情况下，路由器的 OSPF 进程会选取路由器中所有接口中 IP 地址最高的那一个作为路由器的 ID。当网络受到攻击时，如果这个接口崩溃了，则路由器不得不重新选择路由器 ID，然后重新计算路由信息，这样将极大地降低网络的稳定性和收敛速度，并且浪费了路由器大量的内存和 CPU。

如果路由器配置了回环接口后，路由器将优先采用回环接口的 IP 地址作为路由器 ID，从而提高了稳定性。给路由器配置回环接口的方法如下。

```
Router(config)# interface loopback 0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
```

当然，我们还可以直接指定路由器的 ID，也能达到同样效果，方法如下。

```
RouterA(config)# router ospf 100
RouterA(config-router)# router-id 1.1.1.1
```

6. 配置 SPF 计时器

由于网络拓扑通常是相对稳定的，开启 SPF(Shortest Path First，最短路径优先算法，用于 OSPF 路由计算)计时器是合适的，它可以使少数路由器暂时崩溃或者将路由不稳定的区域控制在最小范围。

在 SPF 计时器中有两个参数，一个是 SPF-delay，另一个是 SPF-holdtime。SPF-delay 为延迟时间，单位为秒。它是 OSPF 接受一个拓扑变化和开始一个 SPF 计算的时间间隔。SPF-holdtime 是在两个连续的 SPF 计算之间的最小时间，以秒为单位。在接收到一个拓扑变化时，一个路由器开始它的 OSPF 最短距离重新计算前，SPF 计时器的值能够抑制其立刻进行计算，其配置方法如下。

```
Router(config)# router ospf 100
Router(config-router)# timers spf 10 20
```

虽然这个选项能够增加网络受到攻击时的稳定性，但是因为网络攻击会导致很多路由抖动，这也增加了一个网络受到攻击后再次收敛的时间。这将导致 OSPF 网络的冗余设计比正常情况下将会花费更长的时间才能发挥作用，因此网络管理员必须紧密观察其网络设计，以决定是否需要调整这个参数。

7. 配置 OSPF 路由过滤

在 OSPF 路由协议中，OSPF 区域中可以允许路由器控制路由，并对无效的路由进行过

滤。通常的过滤方式有区域过滤和邻居数据库过滤两种，其配置方式如下。

```
RouterB1(config)# router ospf 100
RouterB1(config-router)# area 2 filter-list prefix-list  AREA2 in
RouterB1(config)#ip prefix-list AREA2 deny 10.10.0.0/24
```

8. 配置实例

在图 4-4 中，小 A 攻击的就是 Router A 和 A 校区学生电脑网络相连的 Fa1/0 接口，因此我们需要将这个接口的路由更新信息关闭，并且在骨干区域设置路由认证，防止非法入侵。对于 A、B 校区而言，设置为端区，并且设置路由过滤，防止小 A 的非法路由注入。

❶ 按照下述方法配置路由器 C。

```
RouterC(config)#interface loopback 0
RouterC(config-if)#ip addr 1.1.1.1 255.255.255.255
RouterC(config-if)#exit
RouterC(config)#router ospf 1
RouterC(config-router)#router-id 1.1.1.1
RouterC(config-router)#area 0 authentication message-digest
RouterC(config-router)#neighbor 2.2.2.2
RouterC(config-router)#neighbor 3.3.3.3
RouterC(config)#interface FastEthernet 0/0
RouterC(config-if)#Description ToRouterA
RouterC(config)#ip ospf network point-to-multipoint non-boardcast
RouterC(config-if)#ip ospf message-digest-key 1 md5 cisco
RouterC(config)#interface FastEthernet 0/1
RouterC(config-if)#Description ToRouterB
RouterC(config)#ip ospf network point-to-multipoint non-boardcast
RouterC(config-if)#ip ospf message-digest-key 1 md5 cisco
```

❷ 按照下述方法配置路由器 A。

```
RouterA(config)#interface loopback 0
RouterA(config-if)#ip addr 2.2.2.2 255.255.255.255
RouterA(config-if)#exit
RouterA(config)#router ospf 1
RouterA(config-router)#router-id 2.2.2.2
RouterA(config-router)#neighbor 1.1.1.1
RouterA(config-router)#neighbor 3.3.3.3
RouterA(config-router)#area 0 authentication message-digest
RouterA(config-router)# area 1 stub no-summary
RouterA(config-router)# area 1 default cost 10
RouterA(config-router)# passive-interface FastEthernet 1/1
RouterAConfig-router)# area 1 filter-list prefix-list  AREAa in
RouterA(config)#ip prefix-list AREAa deny 10.10.0.0/24
RouterA(config)#interface FastEthernet 0/0
RouterA(config-if)#Description ToRouterC
RouterA(config)#ip ospf network point-to-multipoint non-boardcast
RouterA(config-if)#ip ospf message-digest-key 1 md5 cisco
RouterA(config)#interface FastEthernet 0/1
RouterA(config-if)#Description ToRouterB
RouterA(config)#ip ospf network point-to-multipoint non-boardcast
RouterA(config-if)#ip ospf message-digest-key 1 md5 cisco
```

❸ 按照下述方法配置路由器 B。

```
RouterB(config)#interface loopback 0
RouterB(config-if)#ip addr 3.3.3.3 255.255.255.255
RouterB(config-if)#exit
```

```
RouterB(config)#router ospf 1
RouterB(config-router)#router-id 3.3.3.3
RouterB(config-router)#neighbor 1.1.1.1
RouterB(config-router)#neighbor 2.2.2.2
RouterB(config-router)#area 0 authentication message-digest
RouterB(config-router)# area 1 stub no-summary
RouterB(config-router)# area 1 default cost 10
RouterB(config-router)# passive-interface FastEthernet 1/1
RouterBConfig-router)# area 1 filter-list prefix-list  AREAb in
RouterB(config)#ip prefix-list AREAb deny 10.10.0.0/24
RouterB(config)#interface FastEthernet 0/0
RouterB(config-if)#Description ToRouterC
RouterB(config)#ip ospf network point-to-multipoint non-boardcast
RouterB(config-if)#ip ospf message-digest-key 1 md5 cisco
RouterB(config)#interface FastEthernet 0/1
RouterB(config-if)#Description ToRouterA
RouterB(config)#ip ospf network point-to-multipoint non-boardcast
RouterB(config-if)#ip ospf message-digest-key 1 md5 cisco
```

点评与拓展： 在 UT 大学采用 OSPF 网络后，通过对骨干区域进行消息验证，并对接入的 A、B 两个校区都设置为端区获得了较好的路由安全性；对于容易受到攻击的结点，进行了路由过滤，防止攻击产生的非法路由进入校区网络；同时对接入到学生宿舍网络的接口采用了被动模式，小 A 通过抓包将一无所获，甚至连网络上用的什么路由协议都不知道。UT 大学则在网络升级的过程中，获得了更好的路由安全性，并为以后网络升级打好了基础。

4.3 定向组播控制

4.3.1 Smurf 攻击

Smurf 攻击主要基于互联网控制信息包(ICMP)，它是一种强力的拒绝服务(DoS)攻击方法，主要利用的是 IP 协议的直接广播特性，如图 4-6 所示。

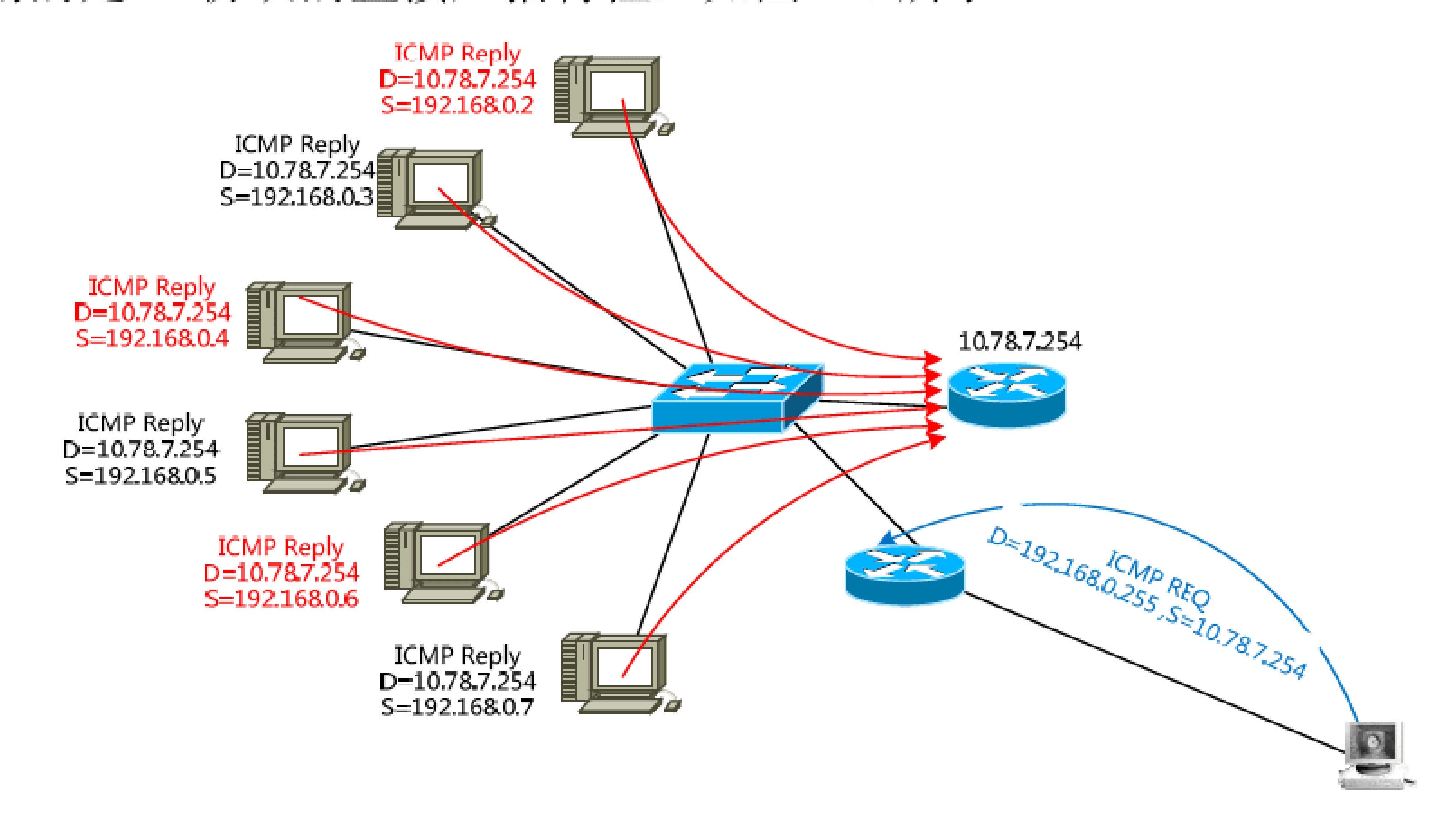


图 4-6 Smurf 攻击

Smurf 攻击的方法如下。

- ✧ 黑客锁定一个被攻击的主机(通常是一些 Web 服务器)。
- ✧ 黑客寻找可作为中间代理的站点，用来对攻击实施放大(通常会选择多个，以便更好地隐藏自己，伪装攻击)。
- ✧ 黑客给中间代理站点的广播地址发送大量的 ICMP 包(主要是指 Ping 命令的回应包)，这些数据包全都以被攻击的主机的 IP 地址作为 IP 包的源地址。
- ✧ 中间代理向其所在的子网上的所有主机发送源 IP 地址欺骗的数据包。
- ✧ 中间代理主机对被攻击的网络进行响应。

假设黑客拥有调制解调器，或者其他能快速上网的方式，能以 1Mbps 的速度向中间代理机器发送 ICMP 数据包；再假设中间代理站点有 150 台主机对这些 ICMP 包作出了响应。这样，一下子就有 150Mbps 的攻击数据从中间代理涌向被攻击的主机。黑客可以控制这个过程直到他自己连接到中间代理机器上，并且控制中间代理持续向被攻击主机发送 ICMP 包。

如果没有必须要向外发送广播数据包的情况，就可以在路由器的每个接口上设置禁止直接广播，防止路由器成为黑客的中间代理，其配置方式如下。

```
Router(config)# interface FastEthernet  0/1
Router(config-if)# no ip directed-broadcast
```

4.3.2　单播逆向路径转发

单播逆向路径转发(Unicast Reverse Path Forwarding，URPF)的主要功能是防止基于源地址欺骗的网络攻击行为。之所以称为“逆向”，是针对正常的路由查找而言的。一般情况下，路由器接收到报文，获取报文的目的地址，针对目的地址查找路由，如果找到了就转发报文，否则丢弃该报文。URPF 通过获取报文的源地址和进入接口，以源地址为目的地址，在转发表中查找源地址对应的接口是否与进入接口匹配，如果不匹配，则认为源地址是伪装的，丢弃该报文。通过这种方式，URPF 能够有效地防范网络中通过修改源地址而进行的恶意攻击行为。图 4-7 所示是一种攻击模型。

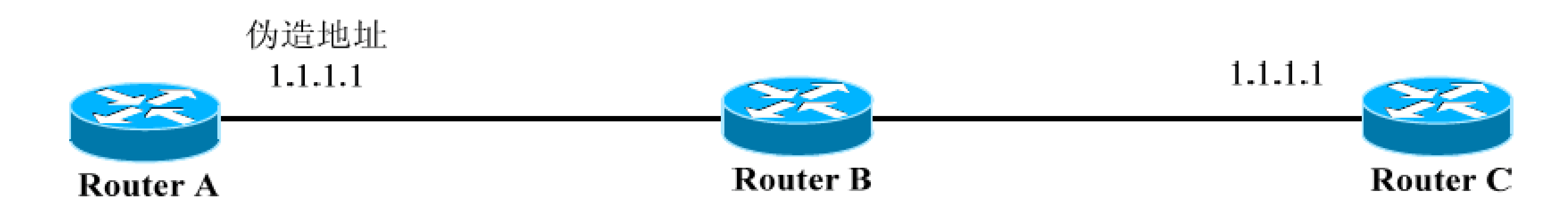


图 4-7　伪造源地址攻击模型

在 Router A 上伪造源地址为 1.1.1.1 的报文，向 Router B 发出请求，Router B 响应请求时将向真正的“1.1.1.1”发送报文。这种非法报文对 Router B 和 Router C 都造成了攻击。受攻击者除了一次一跳地追踪这个分组的来源以外，并没有其他的办法来检测它。在这种情况下，如果站点 B 的网络管理员在其路由器上启用某种类型的机制就可能很好地防范这样的攻击。URPF 技术可以应用在上述环境中，阻止基于源地址欺骗的攻击。

URPF 通过查找任何进入路由器的路由表的接口分组的源 IP 地址工作，从逻辑上，如果这个源地址属于路由器背后的网络并且不是一个受欺骗的地址，这个路由表就包含一个

入口通道，显示路由器有一个通过分组到达的接口去往该地址的途径。但是如果这个地址是一个受欺骗的地址，路由表可能就没有这个入口通道，因此地址不在这个路由器中，而是从 Internet 上某个网络(例如图 4-7 中的 Router C)偷来的，当路由器查找路由时，如果没有发现这个源地址，就丢弃该分组。

Cisco 为了优化 URPF 的速度，使用了 Cisco CEF 快速转发引擎来处理。URPF 则是通过查找 CEF 产生的转发信息数据库，而不是查找路由表。 这样将会更高效地进行工作，因此在配置时必须开启 CEF。图 4-8 显示了 URPF 是如何工作的。

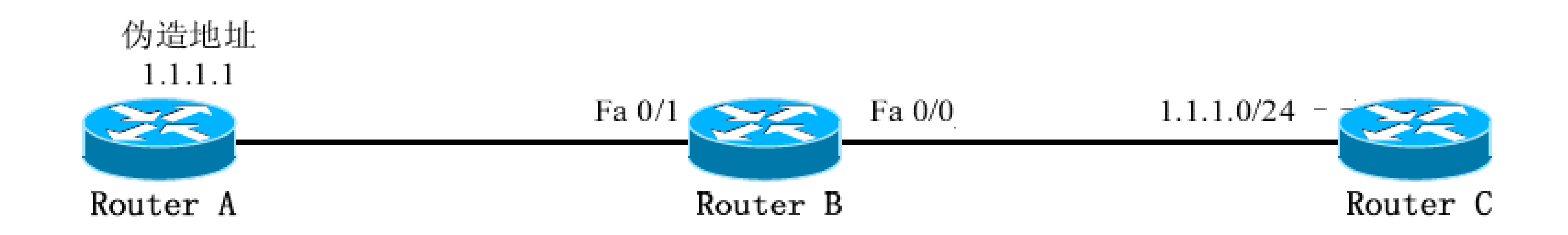


图 4-8 URPF 工作原理

- ✧ 当 IP 分组以源地址 1.1.1.1 到达 Fa0/0 接口时，URPF 做逆向查找来评定这个源 IP 地址，通过查找发现 1.1.1.1 源地址的确来自 Fa0/0 接口，则 URPF 验证通过。
- ✧ 当 IP 分组以源地址 1.1.1.1 到达 Fa0/a 接口时，URPF 做逆向查找来评定这个源 IP 地址，通过查找发现 1.1.1.1 源地址来自 Fa0/0 接口，而非 Fa0/1，则 URPF 验证未通过，丢弃分组。

URPF 的配置方法如下。

❶ 开启 CEF 快速转发，以便 URPF 快速查询转发表。

```
Router(config)# ip cef
```

❷ 在接口上配置 URPF。

```
RouterA(config)#interface FastEthernet 0/0
RouterA(config-router)# ip verify unicast reverse-path
```

点评与拓展：URPF 工作原理虽然简单，但是需要选择合适的路由器进行配置，否则可能在一些路由器上产生不对称路由。所谓不对称路由就是当一个分组发送返回流量通过的接口与接收该分组的原始接口不同。例如某个用户发送接口为 A，但是流量返回的接口是 B，这样的情况很有可能是网络管理员的一个合理的安排，但是如果启动 URPF 后则会导致如上所说的路由不对称问题。因此通常将 URPF 应用在一个网络的边缘上。

4.4 路由黑洞过滤

路由黑洞过滤是一种较为少见的技术，它通过一个名为 Null 0 的接口来代替访问控制列表将非法流量过滤掉。Null 0 接口的作用就是定义一个丢弃报文的接口，通过配置静态路由获得。配置 Null 0 的方法如下。

```
RouterA(config)#ip route 127.0.0.0 255.0.0.0 null 0
RouterA(config)#ip route 192.168.0.0 255.255.0.0 null 0
```

同时，为了避免因流量转储到 Null 0 接口而产生 ICMP 不可达消息被对方攻击者再次



利用，需要在 Null 0 接口上配置禁用 ICMP 不可达消息，配置方法如下。

```
RouterA(config)#interface FastEthernet 0/0
RouterA(config-if)# no icmp unreachables
```

通常，还会加一条管理距离为 255 的默认路由，为没有有效路由的路由器路由所有流量，并且可以避免一些简单的 DoS 攻击以改善性能。但是，加入时必须要将管理距离调整为最大值 255，防止其影响其他管理距离较小的路由条目。同时如果管理员定义了一条管理距离小于 255 的默认路由，该命令也会失效。该配置方法如下。

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 null 0 255
```

4.5　路径完整性检查

在路由协议以一种安全的方法建立起来以后，确保所有流量通过路由协议基于路径最短优先计算出来的路径被路由是重要的。但是，IP 中的一些特性能够改变的只有路由器自己依赖路由协议所作出的路由决定。有两个重要的特性需要我们关注：一是 IP 源路由，另一个是 ICMP 重定向。

4.5.1　IP 源路由

IP 源路由是 IP 的一个特性，它允许用户在 IP 分组中设置一个字段来指定它想要这个分组经过的路径。源路由能够破坏正常路由协议的工作，从而给攻击者留下了一个机会。使用源路由的方法只有几种，其中以松散源记录路由(Loose Source Record Route，LSRR)较为出名。

攻击者可以使用源路由的一个方法从公用网络到达 RFC1918 专用地址空间。正常情况下，这些网络不能通过 Internet 到达，因为 Internet 路由器不知道该怎样路由这些地址。但是攻击者能够使用源路由去告诉路由器怎样处理这些分组。一个攻击者可以指定一个加入公网和专用网络的路由器作为到达中间点。例如，在路由器背后的某个为 192.168.0.2 的文件服务器，正常的情况下，Internet 将无法访问到这样的服务器，但是通过设置源路由，攻击者可以轻易地欺骗路由器，并可能将数据转发给该文件服务器。

如果没有特别的需求，可以在路由器的接口上关闭源路由，方法如下。

```
RouterA(config)#interface FastEthernet 0/0
RouterA(config-router)# no ip source-route
```

4.5.2　ICMP 重定向

在关闭 IP 路由的情况下，路由器还会接收伪造的 ICMP 重定向，远程攻击者可以利用这个漏洞发送恶意 ICMP 信息包而修改路由器中的路由表。

如果路由器的 IP 路由功能关闭，它就会接收伪造的 ICMP 重定向包并修改它的路由表。在 IP 路由关闭的情况下，路由器会作为主机操作。在 IP 路由打开的情况下(默认情况下是打开的)，ICMP 重定向包会接收并辨认，不过 ICMP 重定向包会忽略，路由器不会根据重

定向包更新路由表。下面列举了伪造 ICMP 重定向包的危害：

- 通过发送伪造的 ICMP 重定向包，恶意用户可以破坏或者截获来自路由器上的通信。
- 通过通告本地子网不使用的 IP 地址为默认网关，可以导致路由器发送任意包到本地子网以外的目的地。
- 通过通告网关处于完全不同的子网，如果某一设备为这个伪造的网关代理 ARP 请求，所有目的路径为外部子网的通信会转发到伪造的网关。而如果没有设备为伪造网关代理 ARP 请求，就会出现第一种情况描述的信息被阻挡。
- 恶意用户插入默认网关为攻击者机器的 IP 地址，可以截获所有通信。

避免这样的攻击可以在接口上关闭 ARP 代理请求和 ICMP 重定向功能。一个较好的边界接口配置方案如下。

```
RouterA(config)#interface FastEthernet 0/0
RouterA(config-if)# ip verify unicast reverse-path
RouterA(config-if)# no ip redirects
RouterA(config-if)# no ip directed-boardcast
RouterA(config-if)# no ip proxy-arp
```

4.6 本 章 小 结

本章主要讲述了一些基本的路由器安全配置方案，并通过实例介绍了 RIP 和 OSPF 路由协议的安全防范。在 RIP 协议中，可以屏蔽不用端口的路由更新，并且可以使用 MD5 的方式对路由消息进行认证。OSPF 协议则除了路由消息认证外，还可以提供端区的设置，并在区域内过滤非法的路由条目。随后介绍了一些通过路由黑洞过滤防止简单的 DDoS 攻击的方法，以及通过关闭源路由、ICMP 重定向等进一步提高了路由器安全的方法。对于服务提供商，我们将在后续的章节中介绍 BGP 等协议的使用以及访问控制列表等功能。

第 5 章　交换机及交换网络安全

随着网络的逐渐发展，以太网价格逐渐下降，交换机逐渐拥有多层交换功能，交换式的网络已经在很多公司、企业、院校局域网络中采用。但是构造交换式的局域网在带来众多优点的同时，也带来了很多安全隐患，如广播攻击、MAC 攻击、VLAN 欺骗、ARP 病毒等。如何防范第 2 层的攻击已经成为相当重要的一个问题了。

通过本章的学习，读者应掌握以下主要内容：

✧ VLAN 的定义以及 PVLAN 的实现
✧ 生成树算法的安全
✧ ARP 病毒攻击与防范
✧ MAC 攻击防范

5.1　VLAN 隔离

应用实例导航：Sadness 公司交换网络攻击与防范

※场景呈现

Sadness 公司是一个大型的制造类企业，但是由于其自身发展速度过快而网络建设并未投入太多的精力，仍旧使用局域网共享文件的方式共享数据。某日一工程部人员的投标书在网络传输的过程中被技术部人员 SC 截获，此人将其卖给竞争对手，使得公司丢掉了一笔极大的订单。

当公司丢掉这笔订单后，试图查出泄漏标书的人，却因为这样一个简单的共享型网络查而无终。最终认为是公司外部人员窃取了标书，于是在内部和外部网络之间加装了防火墙。

从这之后，泄漏标书的 SC 多次截获网内报文，继续高价卖出获利，给 Sadness 公司带来了巨大损失。

※技术要领

(1)　VLAN 的基本概念及划分方式；
(2)　交换式网络中 VLAN 的基本配置方法。

VLAN(Virtual Local Area Network，虚拟局域网)是一种将局域网设备从逻辑上划分(注意，不是从物理上划分)成一个个网段，从而实现虚拟工作组的新兴数据交换技术。一方面，VLAN 建立在局域网交换机的基础之上；另一方面，VLAN 是交换式局域网的灵魂。这是

因为通过 VLAN 用户能方便地在网络中移动和快捷地组建宽带网络，而无需改变任何硬件和通信线路。这样，网络管理员就能从逻辑上对用户和网络资源进行分配，而无需考虑物理连接方式。VLAN 充分体现了现代网络技术的高速、灵活、管理简便和扩展容易等特征。是否具有 VLAN 功能是衡量局域网交换机的一项重要指标。网络的虚拟化是未来网络发展的潮流。

VLAN 与普通局域网从原理上讲没有什么不同，但从用户使用和网络管理的角度来看，VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，甚至位于不同的国家。

VLAN 是一种逻辑上的局域网，可以将不同交换机、不同地域的接口划分到一个虚拟的 VLAN 中，便于管理和维护；同时划分 VLAN 还可以隔离广播流量，防止大型网络中多台机器广播影响性能。

对于前述案例，如果 Sadness 公司使用 VLAN 隔离不同部门的流量，则不会出现类似的监听泄密问题了。

5.1.1 VLAN 划分

VLAN 成员模式有两种：静态 VLAN 和动态 VLAN，如图 5-1 所示。前者对应的划分方法是基于端口划分，后者对应的三种划分方法：基于 MAC 地址划分、基于网络地址划分和基于策略划分。

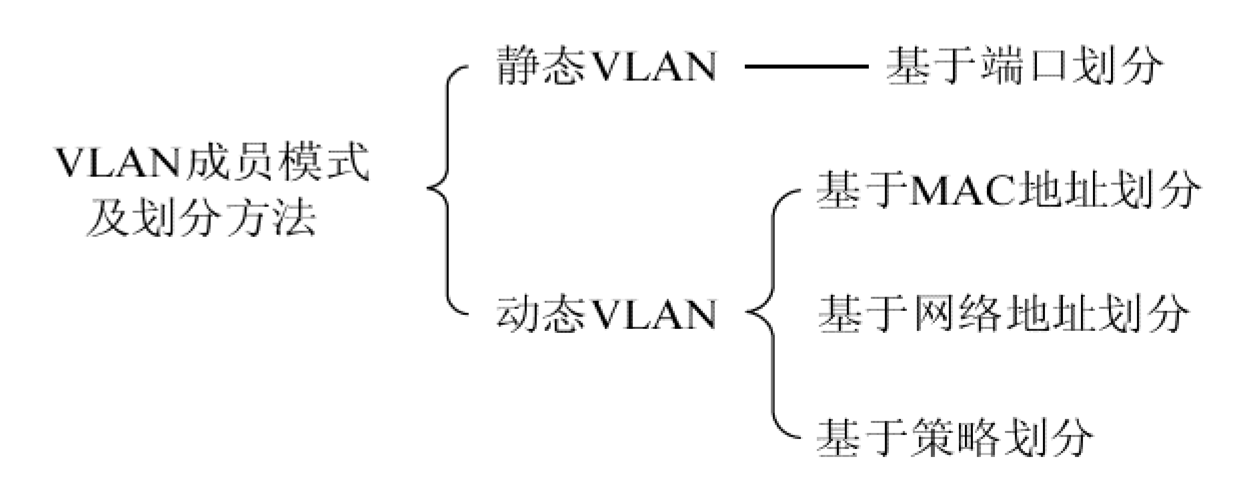


图 5-1 VLAN 成员模式和划分方法

1. 基于端口划分 VLAN

静态 VLAN 或基于端口划分的 VLAN 是最常用的 VLAN 划分方式，网络管理员把交换机的某个端口分配给一个 VLAN 之后，此端口将保持某 VLAN 的成员身份，除非管理员更改其配置。比如某交换机的 1~4、18、20、22 端口为 VLAN 10，5~17 为 VLAN 20，等等。根据端口划分是目前定义 VLAN 最广泛的方法，IEEE 802.1Q 规定了依据以太网交换机的端口来划分 VLAN 的国际标准。

这种划分方法的优点是定义 VLAN 成员时非常简单，只要将所有的端口都指定一下就可以了。它的缺点是当一个用户从一个端口移动到另一个端口时，网络管理员必须对虚拟局域网成员进行重新配置。

2. 基于 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据连接在网络中的每个设备网卡的物理地址来划分

VLAN，即对每个 MAC 地址的主机都配置其属于哪个组。这种划分 VLAN 的方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种方法的缺点是初始化时所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置任务繁重。而且这种划分方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。

Cisco 的交换机可以使用名为 VMPS(VLAN Management Policy Server，VLAN 成员策略服务器)的服务器来创建一个 MAC 地址数据库，并用于动态地管理 VLAN。VMPS 实际上就是一个 MAC 地址到 VLAN 的映射数据库。

3. 基于网络层地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的，虽然这种划分方法是根据网络地址，比如 IP 地址，但它不是路由，与网络层的路由毫无关系。它虽然查看每个数据包的 IP 地址，但由于不是路由，所以没有 RIP、OSPF 等路由协议，而是根据生成树算法进行桥交换。

这种划分方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。另外，这种方法不需要附加的帧标记来识别 VLAN，这样可以减少网络的通信量。

这种划分方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)，一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

4. 基于策略的 VLAN

基于策略的 VLAN 是一种比较灵活有效的 VLAN 划分方法。目前，常用的策略有(与厂商设备的支持有关)：按 MAC 地址、按 IP 地址、按以太网协议类型、按网络的应用等。

划分 VLAN 后的交换机将使用 VLAN 标记，以标明此帧是属于哪一个 VLAN 的。利用这个标记，交换机才能把收到的帧发送到正确的端口。

5.1.2　VLAN 配置

1. 创建 VLAN

创建 VLAN 的方式有两种，一种是全局配置模式下创建 VLAN，另一种是在 VLAN 数据库模式下创建(这种方法仅限于 Cisco 交换机)。

1)　在 VLAN 数据库模式下创建 VLAN

例如，我们现在需要创建一个名为 Jam 的 VLAN，其 VLAN 编号为 3，在 VLAN 数据库模式下创建 VLAN 配置过程如下。

❶ 在交换机的特权模式下，进入 VLAN 数据库模式。

```
Switch#vlan database
```

```
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
Switch(vlan)#
```

❷ 创建 VLAN 3，并将其命名为 Jam。

```
Switch(vlan)#vlan 3 name Jam
VLAN 3 added:
    Name: Jam
```

❸ 创建 VLAN 后，必须退出 VLAN 数据库模式才能使得配置生效。

```
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
```

❹ 如果要查看 VLAN 数据库，可以在交换机的特权模式下使用如下命令。

```
Switch#show vlan
VLAN Name                 Status    Ports
---- ------------- --------- --------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/11, Fa0/12,Gi0/1
                                     Gi0/2
3    Jam                  active
1002 fddi-default             act/unsup
--More—
```

2) 在全局配置模式下创建 VLAN

另一种创建 VLAN 方式是在全局模式配置 VLAN，例如我们要在交换机加入一个名为 Cisco 的 VLAN，其 VLAN 编号为 4，其创建过程如下。

❶ 在交换机的全局模式下，直接执行 vlan 命令就可以进入 VLAN 配置模式，并通过 name 命令来修改 VLAN 的名称。

```
Switch(config)#vlan 4
Switch(config-vlan)#name cisco
```

❷ 创建 VLAN 后，需要退出 VLAN 配置模式才能保存创建的 VLAN。

```
Switch(config-vlan)#exit
Switch(config)#
```

同样，可以通过 show vlan 命令来查看 VLAN 数据库。

2. 删除已创建的 VLAN

删除 VLAN 也有两种模式，一种方法是全局配置模式下删除 VLAN，另一种是在 VLAN 数据库模式下删除(这种方法仅限于 Cisco 交换机)。

在 VLAN 数据库模式下，删除一个 VLAN 如下。

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
Switch(vlan)#no vlan 3
```

```
Deleting VLAN 3...
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
```

在全局配置模式下，只需要执行 no vlan 命令即可删除已创建的 VLAN。

```
Switch(config)#no vlan 4
```

删除 VLAN 后，同样可以通过 show vlan 命令来查看 VLAN 数据库来验证命令执行情况。

3. 指定交换机端口的 VLAN 属性

使用 VLAN 的交换机，其端口分为两种不同的类型，一种是接入端口，可以连接各种网络设备，所有通过这种端口接入的网络设备都是某个 VLAN 的成员。交换机通过这种端口向外发送数据帧之前，会把所有的 VLAN 信息删除。通过这种端口连接的网络设备，只能与同一 VLAN 的成员通信。要与其他 VLAN 成员通信，必须经过路由器对数据包的路由。另一种是 Trunk(中继)端口，允许所有 VLAN 的数据通过。这种端口可以用于交换机到交换机、交换机到路由器，甚至交换机到服务器的连接。Trunk 连接只在百兆或千兆这样的快速连接中使用。不管数据帧属于哪一个 VLAN，都可以通过这种端口发送。

配置好 VLAN 后，我们就需要将交换机的相应端口划分到一个 VLAN 中，其方法如下。

❶ 在交换机的全局配置模式下，进入需要配置 VLAN 的端口。

```
Switch(config)#interface fastEthernet 0/1
```

❷ 将端口的类型修改为接入端口。

```
Switch(config-if)#switchport mode access
```

❸ 指定端口的 VLAN 号。

```
Switch(config-if)#switchport access vlan 3
```

❹ 在新版的 Cisco 交换机中，配置 VLAN 是相当智能化的，当将一个端口加入到没有创建的 VLAN 时，交换机将自动创建相应的 VLAN 号。例如，下面的操作是在交换机中创建一个 ID 为 100 的 VLAN，并将第 2 个快速以太网端口的 VLAN 号指定为该 VLAN。

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
```

❺ 在新版的 Cisco 交换机中，如果要将一批端口同时加入到同一个 VLAN 中，还可以使用 interface range 命令来批量配置端口的 VLAN 号。下面的例子是指定 2～8、11～15 号端口为 VLAN 4 端口。

```
Switch(config)#interface range fastEthernet 0/2 - 8 , fastEthernet 0/11 -
15
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
% Access VLAN does not exist. Creating vlan 4
Switch(config-if)#
```

❻ 配置完成后，需返回到特权模式，并保存配置。

```
Switch (config-if)#end
Switch #copy run start
```

❼ 可以通过 show run 或 show interface 命令来验证配置。

```
Switch #show interface fa0/1 switchport
```

4. 将交换机端口指定为 Trunk 端口

交换机之间互连的端口需要设置为 Trunk 端口。设置时需要做几项工作：一是将当前端口设置为 Trunk 模式，二是指定数据帧的封装形式，三是定义 Trunk 允许的 VLAN。下面的例子是将交换机的 FastEthernet 0/24 端口设置为 Trunk 端口的配置过程。

❶ 在交换机的全局模式下，进入要配置为 Trunk 的端口。

```
Switch(config)#interface fastEthernet 0/24
```

❷ 将端口的类型修改为 Trunk 端口。

```
Switch(config-if)#switchport mode trunk
```

❸ 指定数据帧的封装形式，其中 isl 是 Cisco 专用的 VLAN 封装形式，dot1q 是 IEEE 制定的国际标准。这是可选设置，对于早期的 Cisco 交换机的默认设置是 isl，近几年出厂的 Cisco 交换机的默认设置是 dot1q，非 Cisco 交换机不需要设置此项，只能采用 dot1q。

```
Switch (config-if)# switchport trunk encapsulation { isl | dot1q }
```

❹ 定义 Trunk 允许的 VLAN，all 表示所有，except 表示除此之外都允许。这也是可选设置，默认情况下允许所有 VLAN 通过该端口。

```
Switch (config-if)# switchport trunk allowed vlan {add vlan-list | all | except
vlan-list }
```

❺ 配置完成后，采用同样的方法保存配置和验证配置。

点评与拓展： 采用如上配置后，则可以将 Sadness 公司的网络按照部门的不同分布划分开，这样技术部的 ST 仅能侦听到自己部门的数据，而无法继续侦听其他部门消息了。VLAN 的配置使得整个公司的网络按照部门从逻辑上隔开了。

5.2 动态 VLAN

应用实例导航：Sadness 公司配置安全的动态 VLAN

※场景呈现

Sadness 公司虽然使用了 VLAN 的方式隔离不同部门之间的流量，但是，某日 SC 在利益的驱使下，继续开始监听，他在工程部某个同事病假未来上班之际，将自己的电脑接在同事的端口上，再一次开始监听，如图 5-2 所示。

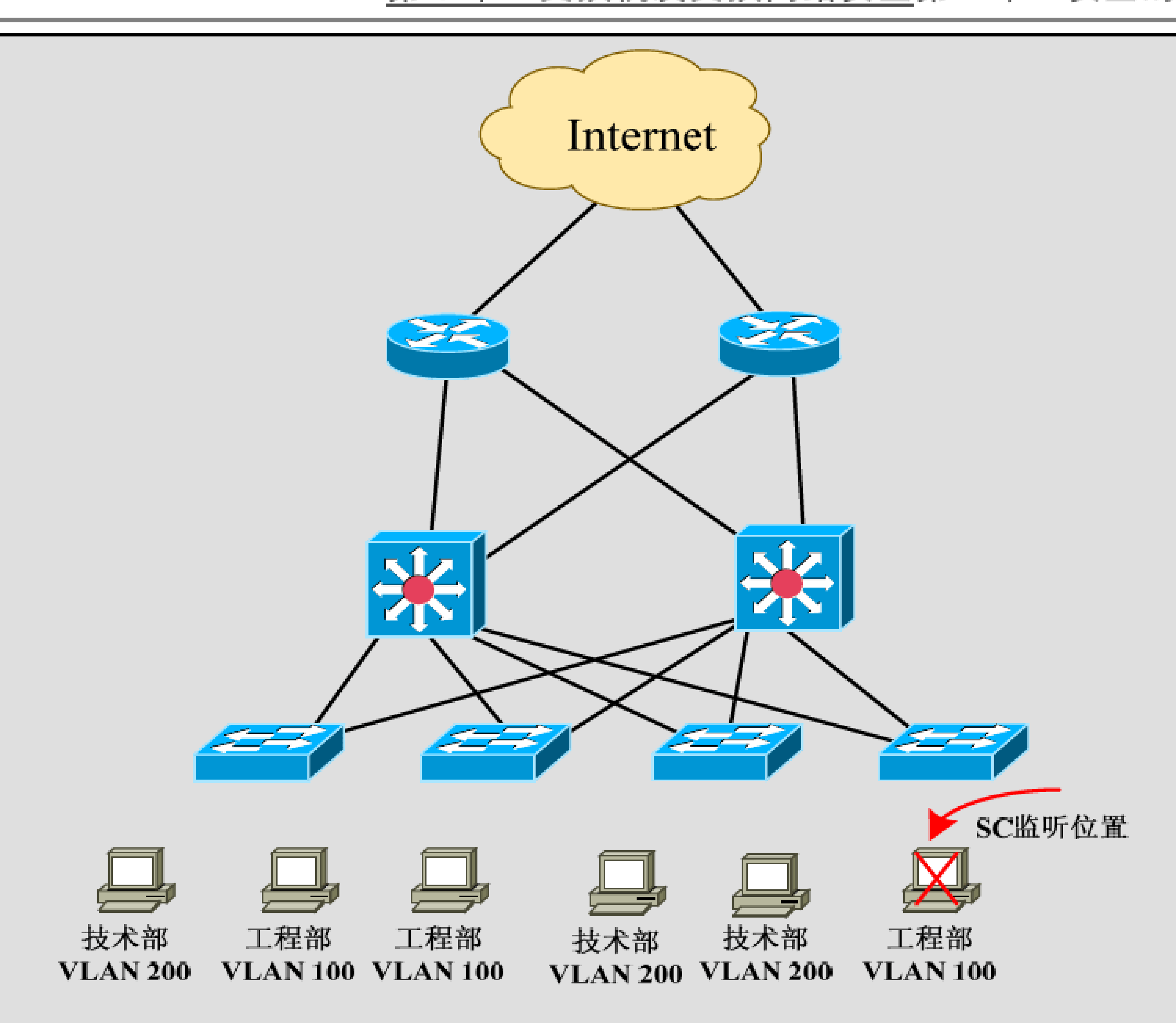


图 5-2　Sadness 公司网络结构图

当公司再次丢掉一笔订单后，却依旧无法查出泄漏标书的人，而泄漏标书的 SC 依旧继续截获网内报文，继续高价卖出标书获利。

※技术要领

(1)　动态 VLAN 的基本原理；

(2)　动态 VLAN 的配置方法。

5.2.1　动态 VLAN 概述

动态 VLAN 的形成很简单，由端口自己决定属于哪个 VLAN 时，就形成了动态的 VLAN。它是一个简单的映射，这个映射取决于网络管理人员创建的数据库。分配给动态 VLAN 的端口被激活后，交换机就缓存初始帧的源 MAC 地址。随后，交换机便向一个称为 VMPS(VLAN Membership Policy Server，VLAN 成员策略服务器)的外部服务器发出请求，VMPS 中包含一个文本文件，文件中存有进行 VLAN 映射的 MAC 地址。交换机对这个文件进行下载，然后对文件中的 MAC 地址进行校验。如果在文件列表中找到 MAC 地址，交换机就将端口分配给列表中的 VLAN。如果列表中没有 MAC 地址，交换机就将端口分配给默认的 VLAN(假设已经定义默认的 VLAN)。如果在列表中没有 MAC 地址，而且也没有定义默认的 VLAN，端口不会被激活，如图 5-3 所示。动态 VLAN 是维护网络安全一种非常好的方法。

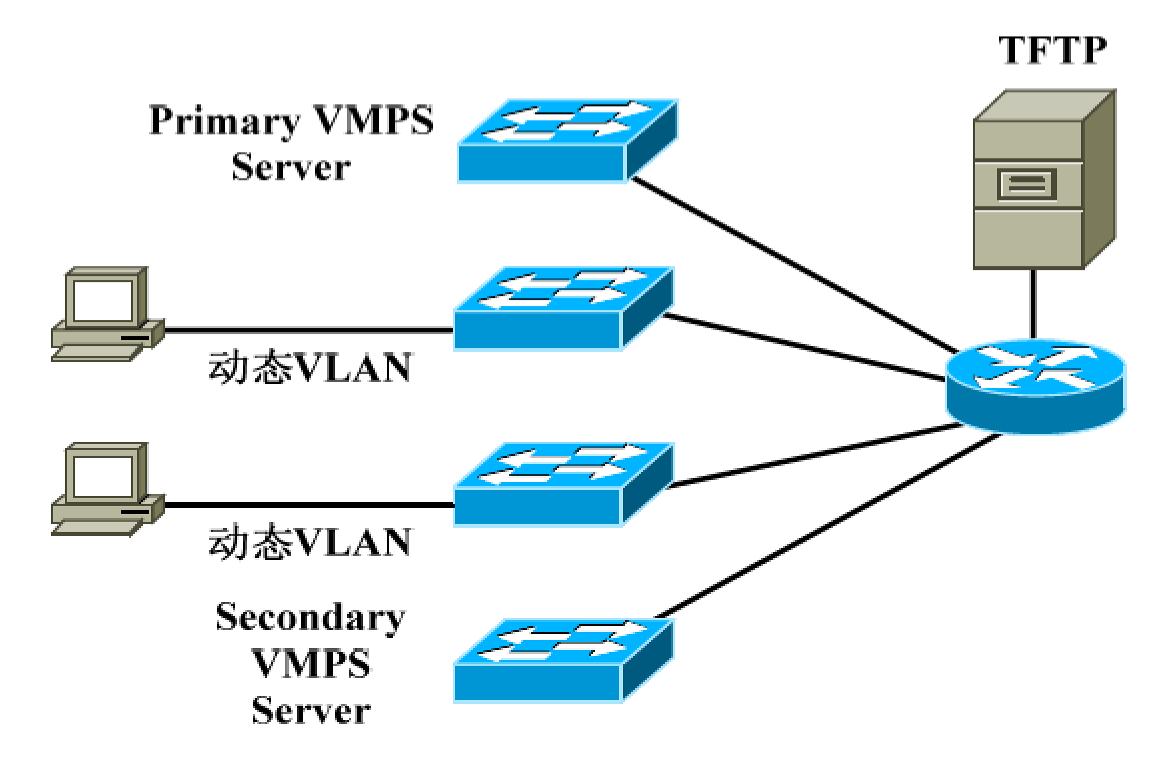


图 5-3 动态 VLAN

如果所分配的 VLAN 被限制在一组端口范围内，VMPS 确认发起请求的端口是否在这个组内，并作如下响应。

✧ 如果 VLAN 在该端口是允许的，VMPS 向客户返回 VLAN 的名字。
✧ 如果 VLAN 在该端口是不允许的，VMPS 不处于安全模式，这时拒绝接入响应。
✧ 如果 VLAN 在该端口是不允许的，并且 VMPS 处于安全模式，VMPS 发出端口关闭响应。

如果 VMPS 数据库内的 VLAN 与该端口上当前的 VLAN 不匹配，并且该端口上有活动主机，VMPS 会视 VMPS 的安全模式发出拒绝或端口关闭响应。如果交换机从 VMPS 服务器端接收到拒绝接入响应，将会阻止由该 MAC 地址发往此端口或者从这个端口发出的数据。交换机将继续监控发往该端口的分组，并在发现新的地址时向 VMPS 或者从这个端口来的通信。如果交换机从 VMPS 服务器接收到端口关闭响应，将会立刻关闭端口，并只能手工重新启用。

出于安全的原因，用户可以配置一个 fallback VLAN 的名字，如果配置连接到网络上并且其 MAC 地址不在数据库中，VMPS 会将 fallback VLAN 的名字发给客户端。如果不配置 fallback VLAN，MAC 地址也不在数据库中，VMPS 将会发出拒绝响应，如果 VMPS 处于安全模式，将会关闭端口。

用户还可以在 VMPS 数据库中显式地添加条目，拒绝待定 MAC 地址的访问。具体方法是将此 MAC 地址对应的 VLAN 名字指定为关键字“-NONE-”。这样，VMPS 就会发出拒绝接入响应或关闭端口。

交换机上的动态端口仅属于一个 VLAN，当链路启用后，交换机只能在 VMPS 服务器提供 VLAN 分配后才会转发来自或者发往此端口的通信，VMPS 客户端从连接到动态端口的新主机发送的首个分组中获得源 MAC，并尝试通过发往 VMPS 服务器的 VQP 请求，在 VMPS 数据库中找到与之匹配的 VLAN。

Cisco Catalyst 2950 和 3550 允许多台同属于一个 VLAN 的主机连接在一个动态端口上。如果活动主机多于 20 台，VMPS 将把接口关闭。如果动态端口上的连接中断，端口将返回隔离状态并且不属于任何一个 VLAN。对连接到该端口的任何主机，在将端口分配给某个 VLAN 之前，要通过 VMPS 重新检查。

5.2.2　配置动态 VLAN

将 VMPS 客户配置为动态时，有一些限制。在为动态端口指定 VLAN 成员身份时采用下面原则。

- ✧ 将端口配置为动态之前，必须先配置 VMPS。
- ✧ VMPS 客户端必须与 VMPS 服务器处于同一个 VTP 管理域中。
- ✧ VMPS 客户端必须与 VMPS 服务器同属于一个管理 VLAN。
- ✧ 如果将端口配置为动态，会自动在该端口启动 STP 的 PortFast 功能。
- ✧ 如果将一个端口由静态配置为同一个 VLAN 中的动态端口，端口会立即连接到此 VLAN 上，直到 VMPS 为动态端口上特定的主机的合法性检查数据库。
- ✧ 静态端口不可以改变为动态端口。
- ✧ 静态的 Trunk 不可以改变为动态端口。
- ✧ EtherChannel 内的物理端口不能被配置为动态端口。
- ✧ 如果有过多的活动主机连接到端口中，VMPS 会关闭动态端口。

1. VMPS 数据库配置文件

VMPS 数据库配置文件必须放置在 TFTP 服务器上，VMPS 数据库配置文件是一个 ASCII 码的文本文件。如下是一个标准的 VMPS 数据库配置文件示例。

```
!VMPS File format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain cisco
vmps mode secure
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
address 5254.AB3B.FC20 vlan-name cisco
address 000A.EB22.057F vlan-name cisco
address 0010.7b7f.790e vlan-name aaa
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name ccc
!
!Port Groups
!
!vmps-port-group <group-name>
```

```
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group JAM
device 192.168.10.199 port 2/1
device 192.168.10.198 port Fa0/5
device 192.168.10.198 port Fa0/6
vmps-port-group "cisco"
device 192.168.10.198 port Fa0/1
device 192.168.10.198 port Fa0/2
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name cisco
vlan-name aaa
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
port-group JAM
vmps-port-policies vlan-name bbb
device 192.168.10.198 port Fa0/9
vmps-port-policies vlan-name Purple
device 192.168.10.198 port Fa0/10
port-group "cisco"
```

由于 VMPS 解析器是基于行的，因此在配置 VMPS 数据库时，要以 VMPS 开头，防止 VMPS 服务器错误地读取其他类型的配置文件。

2. 将交换机配置成 VMPS 服务器

配置完 VMPS 数据库后，则需要配置 VMPS 服务器。通常，VMPS 服务器仅在 Catalyst 5500/6500 等高端交换机上支持，配置方式如下。

```
set vmps downloadmethod rcp | tftp [username]
set vmps downloadserver ip_addr [filename]
set vmps state enable
```

3. 在 Linux 操作系统中配置 VMPS 服务器

当然，中小企业为了使用 VMPS 购买 6500 系列交换机是不值得的。它们如果仅需要 VMPS 功能，可以使用基于 Linux 的 Open VMPSd 软件。VMPSd 软件安装和配置方法如下。

(1) 访问地址http://sourceforge.net/projects/vmps，下载 Open VMPSd。

(2) 在 Linux 中执行 tar-vzxf vmpsd-1.3.tar.gz 命令解压文件。

(3) 执行./configuae 命令配置编译文件。

(4) 执行 Make 命令编译程序。

(5) 执行 Make install 命令安装 Open VMPSd。

(6) 根据上面所述文件配置 vmps 数据库文件。

(7) 运行 vmpsd，其命令是：vmpsd – d – a ip-addr – l 0x0004 – f vmps.db；

(8) 如果需要启动 Linux 服务器时，同时加载 vmps，可以在/etc/rc.local 文件中加入 vmpsd 一行。

4. 将参与动态 VLAN 的交换机配置成 VMPS 客户端

配置完 VMPS 服务器后，需要将参与动态 VLAN 的交换机配置成 VMPS 客户端，其配置过程大致如下。

❶ 在全局配置模式下，指定 VMPS 主服务器地址。

```
Switch(config)#vmps server  <ip地址>  primary
```

❷ 定义 VMPS 备份服务器地址，可以同时定义三个备份服务器。

```
Switch(config)#vmps server <ip地址1>
Switch(config)#vmps server <ip地址2>
Switch(config)#vmps server <ip地址3>
```

❸ 将交换机端口配置为动态 VLAN 模式。

```
Switch(config)#interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
```

❹ 用户还可以通过下述命令来验证 VMPS 客户端的配置。

```
vmps reconfirm minutes                //重新配置时间间隔
vmps retry number-of-retries          //重试次数
clear vmps server                     //清除vmps服务器
clear vmps statistics                 //清除vmps统计
show vmps                             //查看vmps状态
```

至此，我们完成了 VMPS 的配置，如果有新的员工加入公司，则只需要修改 VMPS 数据库即可完成动态分配任务。

📖**点评与拓展：** 采用如上配置后，则可以将 Sadness 公司的网络按照不同的员工和不同的设备划分开，因此数据安全更能得到保证。而且，当非法入侵者将自己的设备接入到其他网络后，网络端口会因为非法入侵而自动关闭，获得了较好的安全性，并且将入侵者的 MAC 地址记录到相应的数据库中，完成攻击者查找的任务。

5.3　安全的 VTP 协议

应用实例导航：Sadness 公司部署安全的 VTP

※场景呈现

使用动态 VLAN 的方式进行 VLAN 分配，但是忽略了交换机之间的链路防范，这次 SC

将魔掌伸向了交换机之间的链路。

为了方便配置 VLAN，Sadness 公司采用了 VTP 协议来同步 VLAN 数据库，但是他们并没有对 VTP 服务进行安全防范。这样 SC 可以将自己的入侵设备模拟成一个中继线接口来和交换机通信，通过 VTP 获得 VLAN 信息，并截取相应的流量，如图 5-4 所示。这次攻击再次让 Sadness 公司丢掉一笔订单，带来了极大的经济损失。

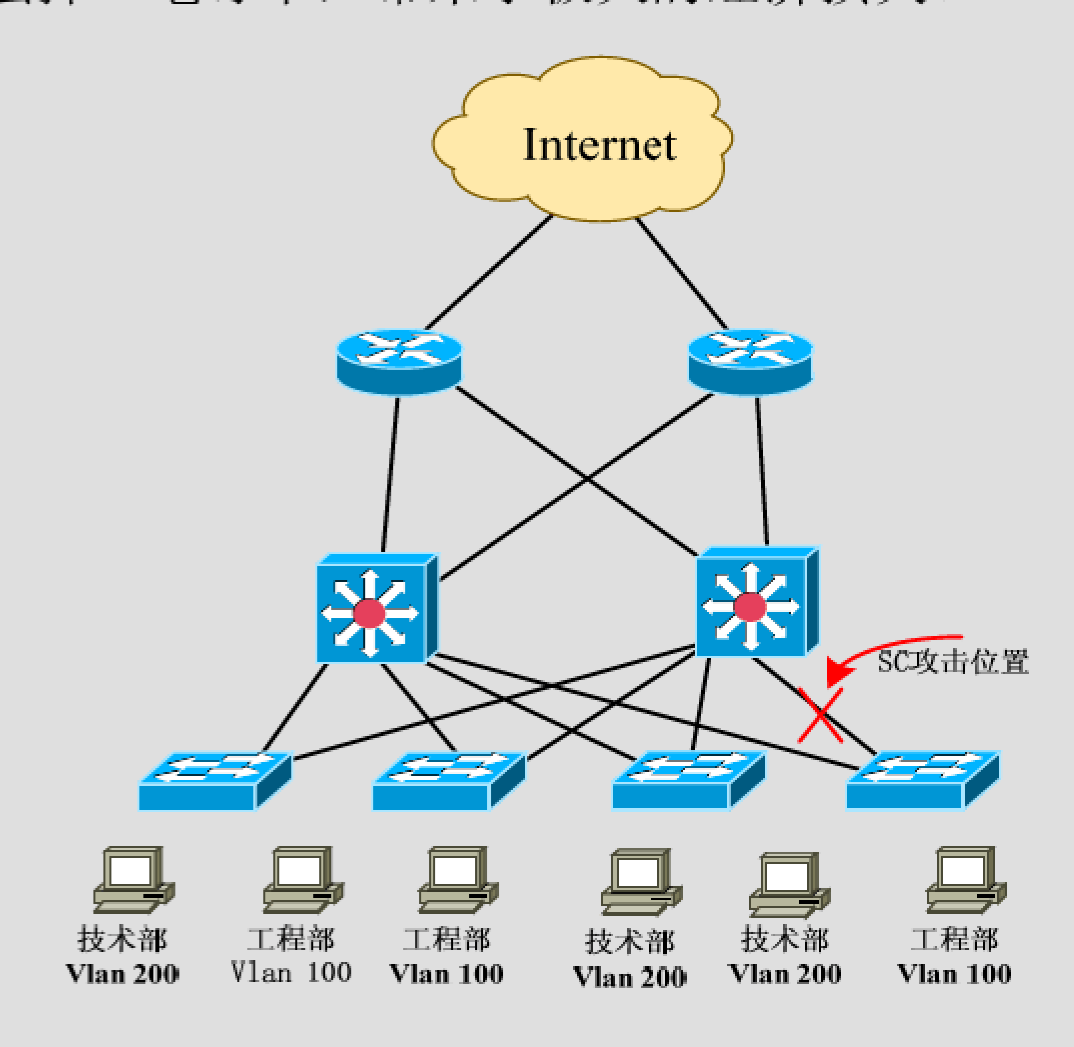


图 5-4　SC 攻击示意图

※技术要领

(1)　VTP 工作原理；

(2)　VTP 的安全配置方法。

5.3.1　VTP 概述

VTP(VLAN Trunking Protocol，VLAN 中继协议)是 Cisco 设计的，用于通过交换机网络进行 VLAN 的管理和配置，并维护 VLAN 配置的一致性。VTP 协议是一个广播 VLAN 配置信息的消息系统，可把 VLAN 配置信息维持在一个管理域(VTP 域)内。VTP 协议使管理员可以在一台交换机上添加、删除或者修改 VLAN，然后同步到其他所有的交换机上，从而在整个网络上维持 VLAN 配置的一致性。虽然 VTP 的方式带来了简便的配置特性，但是不当的使用将再次导致安全隐患。

1.　VTP 工作模式

在一个 VTP 环境里，一台交换机可以是以下 3 种不同的角色，可以是一台 VTP 服务器、一台 VTP 客户机或者工作在透明模式。角色决定了交换机在VLAN 网络中应该被如何配置。在同一个本地网络可以有多个 VTP 域，每个 VTP 域的客户交换机从该域的 VTP 服务器接收自身的配置信息。

1)　VTP 服务器模式

VTP 服务器是每个 VTP 域的根本。服务器是 VTP 域内唯一可以增加、删除、重命名VLAN的交换机。当一台未经配置的 Cisco 交换机第一次上电开机的时候，它的默认模式是服务器模式，用户必须把它修改成客户机或者透明模式。

VTP 服务器周期性地广播 VTP 域名、VLAN 配置，提供现行的配置版本号。这个配置版本号修改号是 VTP 域的一部分，它确保 VTP 域内的所有交换机有现行的、正确的VLAN配置信息。

当VLAN在 VTP 服务器上被创建的时候，和其他VLAN配置信息一起存储在服务器的NVRAM。当交换机重启的时候，配置信息仍被保留。

2)　VTP 客户机模式

VTP 客户交换机从 VTP 服务器接收所有客户交换机的配置信息。客户交换机不能删除、添加、重命名VLAN。当客户交换机加入一个新的 VLAN，VLAN 必须被添加到 VTP 服务器上面去。这样新的VLAN才能传递到所有的客户交换机。当新的VLAN增加后，客户交换机上的端口会关联到新的VLAN。

类似 VTP 服务器，客户交换机在 NVRAM 存储VLAN配置。然而，不像 VTP 服务器，当客户交换机重启的时候，所有的VLAN配置信息丢失了。交换机启动完成后，需要发送一条 VTP 请求消息给 VTP 服务器，来获取现行的VLAN配置。

3)　VTP 透明模式

VTP 透明交换机与 VTP 客户交换机不同，VLAN 可以在这些交换机上手工配置 VLAN。如果配置为 VTP 域的一部分，它们可以从 VTP 服务器接收VLAN配置信息。然而，它们不会通知 VTP 域配置本地的VLAN。

在 VTP v2 中，配置为透明模式的交换机将在 Trunk 端口上转发 VTP 信息以保证其他交换机接收到更新信息，但这些交换机将不修改自己的数据库，也不发送指示 VLAN 状态发生变化的更新信息。在 VTP v1 中，透明模式的交换机也不转发 VTP 信息到其他交换机。需要注意的是透明模式下的交换机可以在本地创建 VLAN，但这些 VLAN 的变化信息不会扩散到其他交换机。

2. VTP 特点

VTP 能够减少在配置改变时可能引起的配置不一致问题的可能性。这种不一致可能会引起安全问题，因为 VLAN 重名会引起交叉连接问题。如果由一种 LAN 类型映射到另一种类型，比如 ATM LANE ELAN 或者 FDDI 802.10 VLAN，则 VLAN 内部可能根本无法连通。VTP 提供一种映射机制，支持部署在混合介质的网络中进行无缝的中继链路。VTP 具有如下优点。

✧　VLAN 配置在整个网络中不变。
✧　在混合介质的网络中允许一个 VLAN 被中继的映射机制。
✧　对 VLAN 的精确跟踪和监控。
✧　全网范围内增加 VLAN 的动态报告。
✧　支持添加新 VLAN 的即插即用配置。

当然，VTP 也有一些缺点，通常与 STP 有关，最大的危险在于桥接环路会跨越整个园

区网进行传播。默认情况下，Cisco 交换机采用 PVST+的生成树协议，每个 VLAN 维持一个 Spanning Tree 实例，而 VTP 又在整个园区 LAN 上传播 VLAN 信息，VTP 就更有可能产生桥接环路。网络设计者和管理员必须在 VTP 带来的易于管理性和可能会产生的不稳定的 STP 域这两者间作出平衡。

5.3.2 配置 VTP 协议

在交换机上创建可以被 VTP 传播出去的 VLAN 之前，先要建立 VTP 域，网络的一个 VTP 域是由一组 VTP 域名字相同并通过 Trunk 链路相互连接的交换机，并且在同一个域中所有交换机共享 VLAN 信息，并且交换机仅能加入到唯一一个 VTP 管理域中。

根据交换机在 VTP 域的角色，需要对 VTP 的模式进行配置。配置内容包括：VTP 域名、VTP 模式、VTP 版本号、VTP 裁剪、VTP 口令和 VTP 陷阱等。

1. 将交换机配置成 VTP 服务器

在一个 VTP 域中，将一台交换机配置成 VTP 服务器模式的方法如下。

❶ 在一个已经建好的 VTP 域中加入一台新的交换机时，需要首先删除交换机上 vlan.dat 和 startup-config，防止残留 VLAN 或者更大的配置版本号带来的问题。

```
Switch#delete vlan.dat
Switch#erase startup-config
```

❷ 确定交换机的 VTP 工作模式为 Server 模式，并且配置 VTP 域名。

```
Switch#vlan database
Switch(vlan)#vtp server
Switch(vlan)#vtp domain cisco
```

❸ 配置 VTP 版本号，这是一个可选配置。VTP 有 1 和 2 两个版本，默认的版本是 2。需要注意在一个 VTP 域中，所有交换机的 VTP 版本应当一致，否则会出现问题。

```
Switch(vlan)#vtp version 2
```

或

```
Switch# vtp version 2
```

❹ 为了保证 VTP 的安全，可以在整个 VTP 域中设置一个管理密码，只有密码正确的 VTP 客户端才能从 VTP 服务器获取 VTP 更新。

```
Switch(vlan)#vtp password  sandnesss
```

或

```
Switch#vtp password  sandnesss
```

❺ 配置 VTP 裁剪。由于主干线路承载了所有 VLAN 的流量，但有些流量可能不必广播到无需运载它们的链路上。VTP 裁剪使用 VLAN 通告决定什么时候该主干连接不需要泛洪式的传输。默认的情况下，主干连接运载此 VTP 管理域中的所有 VLAN 流量，而在实际工作中，有些交换机不必将本地端口配置到每个 VLAN 中，这样启用 VTP 裁剪就成为必要。

```
Switch(vlan)#vtp pruning
```

或

```
Switch#vtp pruning
```

❻ 通过如下命令可以验证 VTP 配置。

```
Switch#show vtp status
VTP Version                           : 2
Configuration Revision                : 3
Maximum VLANs supported locally          : 1005
Number of existing VLANs              : 8
VTP Operating Mode                    : Server
VTP Domain Name                       : cisco
VTP Pruning Mode                      : Disabled
VTP V2 Mode                           : Disabled
VTP Traps Generation                  : Disabled
<….more….>
```

2. 将交换机配置成 VTP 客户机

在一个 VTP 域中，将其他交换机配置成 VTP 客户机的方法如下。

❶ 确定交换机的 VTP 工作模式为 Client 模式，并且配置与 VTP 服务器一致的 VTP 域名。

```
Switch#vlan database
Switch(vlan)#vtp Client
Switch(vlan)#vtp domain cisco
```

❷ 配置与 VTP 服务器一致的 VTP 版本号。如果 VTP 域采用版本 2，可不配置。

```
Switch(vlan)#vtp version 2
```

或

```
Switch# vtp version 2
```

❸ 配置与 VTP 服务器一致的管理密码，只有密码正确才能从 VTP 服务器获取 VTP 更新。

```
Switch(vlan)#vtp password  sandnesss
```

或

```
Switch#vtp password  sandnesss
```

❹ 通过 show vtp status 命令验证 VTP 配置。

5.4 安全的 STP 协议

应用实例导航：Sadness 公司部署安全的 STP

※场景呈现

STP 虽然可以自动避免网络环路，但是其工作方式如果配置不当被黑客利用将会导致全网中断。SC 对 Sadness 的攻击不仅是在 VTP 协议上，还利用了生成树协议的漏洞来进行攻击。攻击者在交换机之间的链路上，通过发送虚假的 STP 消息，从而抢占 STP 的管理权

限，使网络不停地中断，如图 5-5 所示。

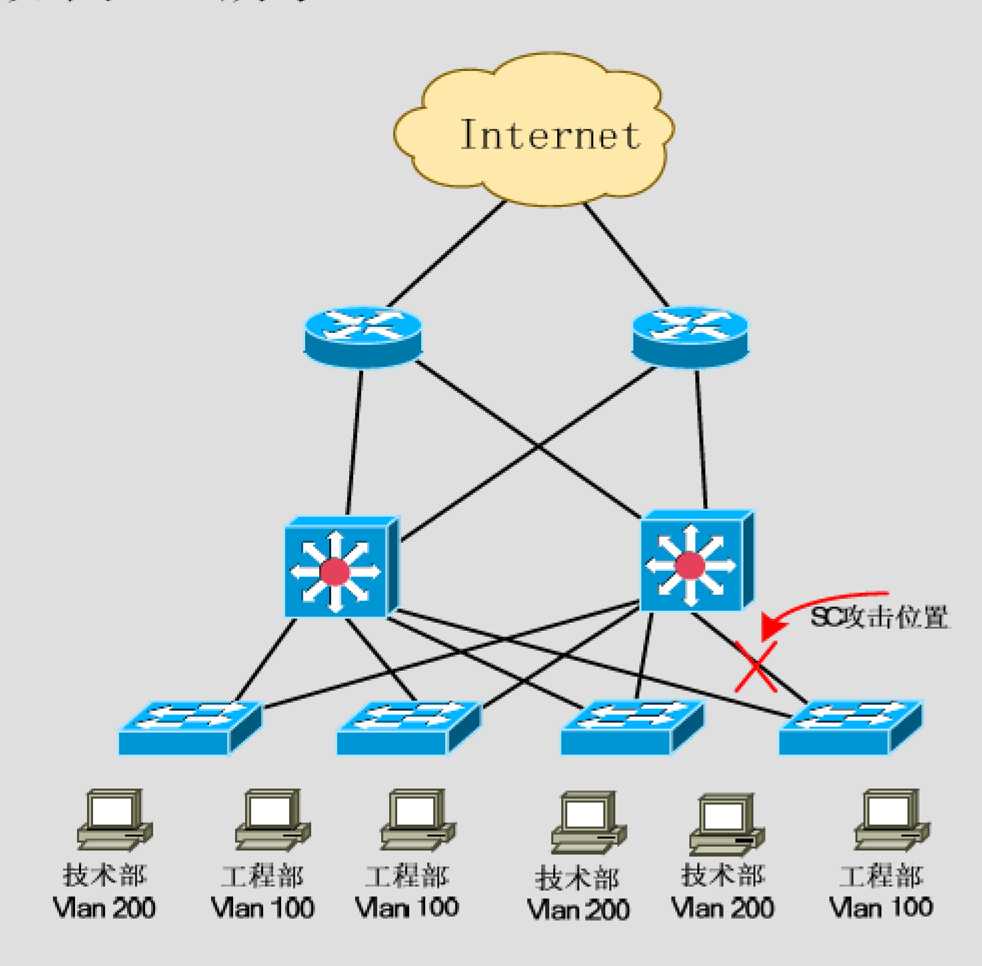


图 5-5　SC 攻击示意图

※技术要领

(1)　STP 的工作原理；
(2)　STP 的保护方法。

5.4.1　STP 协议概述

STP(Spanning Tree Protocol，生成树协议)是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。由于生成树协议本身比较小，所以并不像路由协议那样广为人知，但是它却掌管着端口的转发大权——“小树枝抖一抖，上层协议就得另谋生路”。真实情况也确实如此，特别是在与别的协议一起运行的时候，生成树协议就有可能中断其他协议的报文通路，造成种种奇怪的现象。

如图 5-5 所示的这样一个高冗余度的网络，如果没有 STP 的存在，将会产生大量的广播环路，严重影响性能。生成树协议与其他协议一样，是随着网络的不断发展而不断更新换代的。在生成树协议的发展过程中，旧的缺陷不断被克服，新的特性不断被开发出来。

STP 算法主要依靠 BID(网桥 ID)、路径开销和端口 ID。在创建一个无环路的拓扑时，STP 执行如下 4 个步骤。

(1)　选取根交换机。
(2)　计算到根交换机的最小路径开销。
(3)　确定最小发送者 BID。
(4)　确定最小的端口 ID。

为了作出最佳判决，STP 需要保证所有参与的网桥都获得正确的信息，网桥间的信息交互采用网桥协议数据单元(Bridge Protocol Data Unit，BPDU)的基于 2 层的帧来传递 STP 信息。网桥通过以上 4 步来选择每个端口上所看到的“最佳”BPDU。当一个网桥被激活后，

其所有的端口每隔 2s(默认 Hello 时间)发送一次 BPDU 报文 。如果收到其他端口比自己更好的 BPDU，则本地端口停止发送 BPDU。如果 20s(默认最大时间)的时间没有从邻居收到更好的 BPDU，则本地端口将重新发送 BPDU。最大生存时间是最佳 BPDU 超时的时间。

5.4.2　配置 STP 协议

在实际网络环境中，经常有些用户有意或无意将未经允许的交换设备串接至用户端口，新增交换机的 BPDU 信息可能会导致整个网络第二层网络逻辑拓扑结构变化，引起网络架构震荡；更为严重的是，黑客可能假冒第二层 SPT 信息包冲击甚至改变整个网络二层结构，夺取网络 SPT 中 Root 的位置，使得网络无法正常工作。

在 STP 的实现过程中，可以采用多种措施来防止攻击。

1. PortFast

STP PortFast 是 Cisco Catalyst 系列交换机的一个重要特性，能使交换机或中继端口跳过侦听学习状态，立即进入 STP 转发状态。在基于 IOS 的交换机上，PortFast 只能用于连接到终端工作站的接入端口上。

当一个设备连接到一个端口上时，端口通常进入侦听状态。当转发延迟定时器超时后，进入学习状态；当转发延迟定时器第二次超时，端口进入转发或者阻塞状态；当一个交换机或中继端口启用 PortFast 后，端口立即进入转发状态，但交换机检测到链路，端口就进入转发状态(插电缆后的 2s)；如果端口检测到一个环路同时又启用了 PortFast 功能，它就进入阻塞状态。需要注意的是，PortFast 值在端口初始化的时候才生效，如果端口由于某种原因又被迫进入阻塞状态，随后又需要回到转发状态，仍然要经过正常的侦听和学习过程。

启用 PortFast 的主要原因是防止启动周期小于 30s 的 PC 需要和交换机端口从未连接状态进入到转发状态，一些网卡直到 MAC 层软件驱动被实际加载之后才会启动链路。这种情况下就会导致一些故障，例如 DHCP(动态主机配置协议)环境下，这可能会出现一些问题。

将一个交换机的端口配置成 PortFast 的方法如下。

```
Switch(config-if)#spanning-tree portfast
```

2. UplinkFast

在 STP 收敛过程中，一些终端站点可能会不可达，这主要取决于站点所连接交换机端口的 STP 状态而定。这时会打乱网络连接，关键是减少 STP 的收敛时间和网络受影响的时间。

当链路或交换机发生故障，或 STP 重新配置后，UplinkFast 可以快速选择一个新的根端口。根端口立即进入转发状态，UplinkFast 通过减少最大更新速率来限制突发流量，定义更新分组发送的最大速率，默认为 150 分组/分钟。

UplinkFast 对于网络边缘布线间的交换机非常有用，它不适用于骨干设备。UplinkFast 在直连链路发生故障后提供快速的收敛能力，并通过上行链路组在冗余。

如图 5-5 所示，A 和根交换机相连的端口为转发状态，另一个为阻塞状态。当到根交换机的上行链路断开后，如果配置了 UplinkFast，到另一台上层交换机的链路将直接转入转发

状态。受 UplinkFast 的影响，这个变化将花费 1～5s。一点交换机将以个备用端口转为转发状态，交换机开始在该端口发送伪多播帧，本地桥接标中每个表项都对应一个伪多播帧。它适用工作站地址作为源地址， 01-00-0C-CD-CD-CD 作为目的地址。

如果原来的交换机恢复连接，交换机在等待 2 倍转发延迟时间再加上 5s 后才将该端口转入转发状态。这使得邻接端口有时间经过侦听和学习状态转入转发状态。

配置方法如下。

```
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#spanning-tree uplinkfast
Switch(config-if)#exit
Switch(config)#[no]     spanning-tree     uplinkfast     [max-update-rate
max_update_rate]
Switch#show spanning-tree uplinkfast
```

3. BackboneFast

BackboneFast 是 Catalyst 交换机在根端口或阻塞端口从指定网桥收到一个劣质的 BPDU 时会启动的一种特性。当一个交换机收到一个劣质 BPDU，就以为该交换机的一个非直接链路出现故障。也就是说，一个指定网桥已经丢失到根交换机的连接。按照 STP 规则，因为所有配置的最大生存时间，交换机会忽略所有劣质的 BPDU。

为了减少这 20s 的时间，设计了 BackboneFast 特性。当一个交换机收到劣质 BPDU 的时候，交换机试图判断是否有一条备用路径到根交换机。有以下两种情况。

- ✧ 如果劣质 BPDU 到达一个阻塞端口，则交换机上的根端口和其他阻塞端口成为到根交换机的备选路径。
- ✧ 如果劣质 BPDU 到达根端口，所有的阻塞端口都会成为到根交换机的潜在备用。

如果劣质 BPDU 到达根端口，而且没有阻塞端口，交换机将自己定义为根交换机。如果交换机存在备用路径，它使用备用路径传送一种新的协议，通常情况下该模式会节约 20s 的时间。

如图 5-6 所示，当 L1 Down 时，交换机 B 会发送一个劣等 BPDU，告诉交换机 C，交换机 B 是 Root，交换机 C 经过和交换机 A 沟通(使用 Root Link Query BPDU 查询)，交换机 A 告诉交换机 C，交换机 A 还活着呢。然后交换机 C 告诉交换机 B，交换机 A 还活着，它还是 Root。

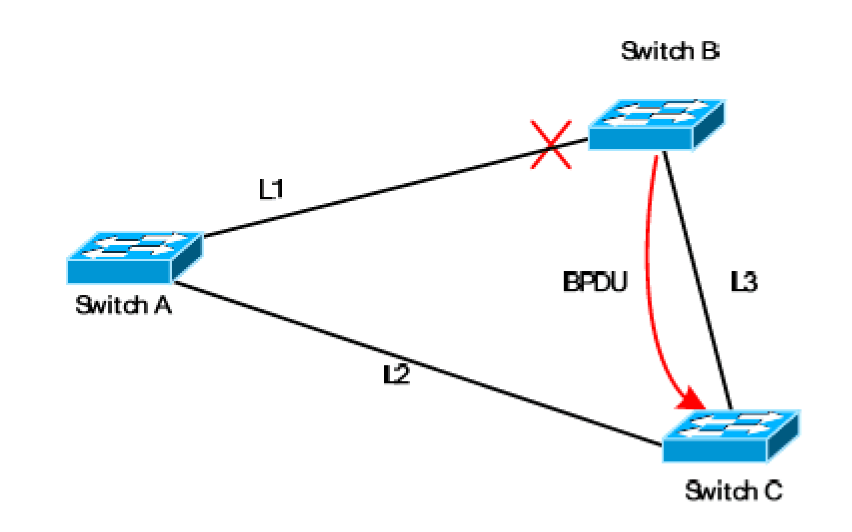


图 5-6 Backbone Fast

配置 BackboneFast 的方法如下。

```
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#spanning-tree backbonefast
```

4. BPDU 保护

BPDU 保护仅用在 PortFast 模式。它被网络设计者用来加强 STP 域边界，从而保持与其的活动拓扑。在启用 STP PortFast 端口之后的设备被禁止影响 STP 拓扑。通过配置 BPDU 保护后，端口如果收到 BPDU 将会把端口状态调整到 Err-Disable。如下是一个出错信息。

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast
enable port. Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

如图 5-7(a)所示，交换机 A 的优先级为 10，是该 VLAN 的根桥，交换机 B 的优先级为 20，为备份根桥，B 和 A 之间的链路为 Gbp/s 链路，是正确的 BPDU 流向。

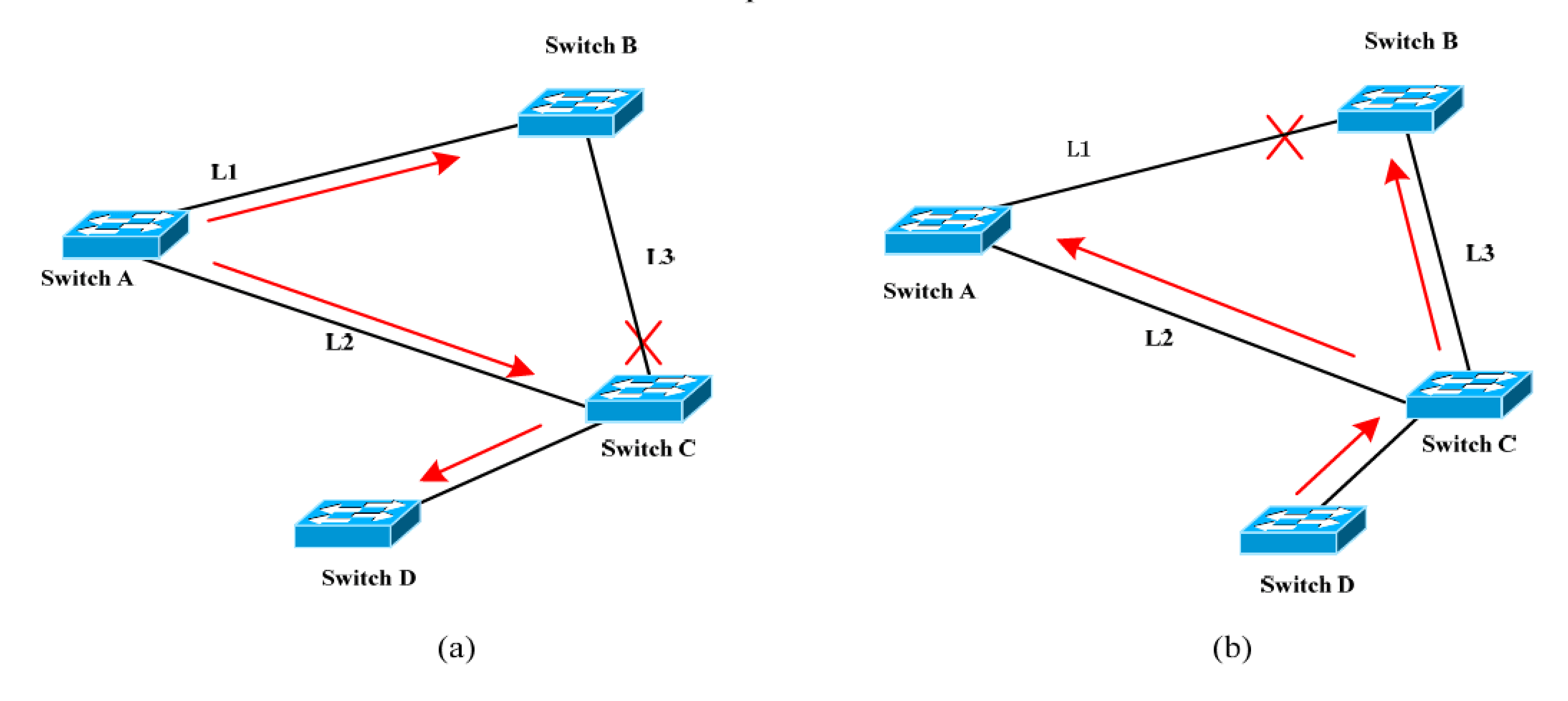


图 5-7　BPDU 保护

如果交换机 D 为一台基于 Linux 的软件网桥，可以发送 BPDU 报文，并将自身 BID 的优先级设置为 0，此时，交换机 D 将成为根桥，故 BPDU 流向变为(b)图，交换机 A、交换机 B 间的 Gbp/s 链路被阻塞，通过交换机 C 走 100Mbp/s 链路。此时会超负载出现丢包的情况，BPDU 保护的目的就是基于这种情况，防止接入设备对整个网络拓扑的影响。

实施 BPDU 保护的配置方式：

```
Switch(config)#spanning-tree portfast bpduguard default  //全局启用BPDU保护
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#spanning-tree bpduguard enable           //在接口上启用
PortFast
```

点评与拓展： *在全局模式配置了 PortFast，默认打开 BPDU 保护，需要在相应的接口上打开 PortFast 才能启用。*

5. 根保护

传统的 802.1D STP 没有给网络管理员提供交换式第 2 层网络拓扑安全。当新接入的交换机优先级更低，将抢占原有的根网桥。

根保护的目的是确保启用了根保护的端口成为指定端口。通常一个根网桥的所有端口

均为指定端口，除非连接到两个或多个根网桥的端口。如果网桥在启用根保护的端口上收到一个较好的 STP BPDU。这个端口进入 STP 的根不一致状态，不会有流量通过该端口。

如图 5-8 所示，交换机 A 和交换机 B 为分布层交换机，交换机 C 为接入层交换机，根为交换机 A。当在交换机 C 下面再接一台交换机时，由于交换机 D 的优先级或 MAC 地址可能比其他要低，可能会使交换机 D 成为根交换机，从而使得从交换机 A 到达交换机 B 的流量不能直接发送到交换机 B，而得使用交换机 C 来转发，这样很不合理(交换机 A 和交换机 B 之间为千兆)。为了避免这种情况，可以在交换机 C 的下联端口上使用根保护，以防止该端口成为根端口，从而防止交换机 D 成为根交换机，确保交换机 A 永远为根交换机。使用根保护后，当交换机 D 接入网络后，交换机 C 的下联交换机 D 的端口会收到一个更新的 BPDU(前提是交换机 D 的优先级最高)，交换机 C 将该端口转为阻塞状态，直到交换机 D 不再发送新的 BPDU 或更改交换机 D 的优先级。

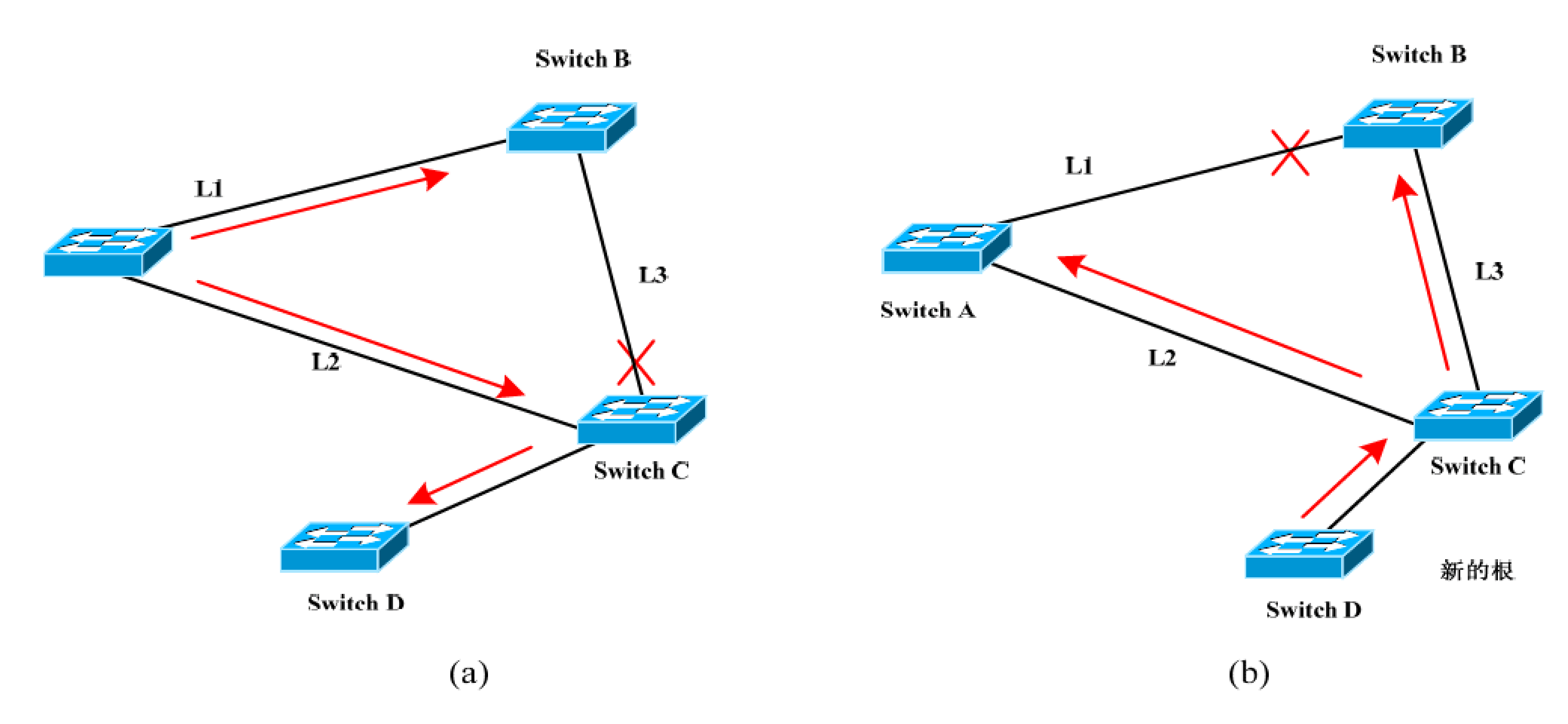


图 5-8　根保护

当一个根保护端口阻塞一个端口时，控制台将会显示如下消息。

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN
77. Moved to root-inconsistent state
```

配置根保护端口的方法如下。

1. 在全局模式下，启用根保护功能。

```
Switch(config-if)#spanning-tree bpduguard enable
```

2. 在需要启用根保护功能的端口上，使用如下命令。

```
Switch(config-if)#spanning-tree guard root
```

3. 用户可以通过如下命令显示端口不一致状态(即为 Block 的端口)。

```
Switch#show spanning-tree inconsistentports
```

点评与拓展： BPDU Guard 技术在交换机端口上启用后，一旦收到其他交换机的 BPDU 信息，此端口立刻防止接口连入交换机，而且必须由网络管理员手工恢复。根保护技术则是在 DP 端口上实现后，该端口就不会改变，只会是 DP 了，这样可以防止新加入的交

换机成为根，该端口就变成了永久的 DP 了。若新加入的交换机想成为根，则它的端口将不能工作，直到这个新交换机委曲求全做 RP 为止。这两个简单的二层 SPT 保护功能，完全防范了不明交换设备的“非法”接入，保证了整个网络交换架构的稳定可靠，是网络自身安全的重要保护手段。

5.5　PVLAN

应用实例导航：为 UT 大学的 IDC 配置 PVLAN

※场景呈现

UT 大学的数据中心(IDC)为学校的众多单位提供主机托管业务，构成了一个多客户的服务器群结构，每个托管客户从一个公共数据中心的一系列服务器上提供 Web 服务。在这个应用中，数据流量的流向几乎都是在服务器与客户之间，而服务器间的横向的通信几乎没有；相反，属于不同客户的服务器之间的安全就显得至关重要。为了保证托管客户之间的安全，防止任何恶意的行为和 Ethernet 的信息探听，需要将每个客户从第二层进行隔离。原先，该 IDC 采用的方法是，使用 VLAN 技术给每个客户分配一个 VLAN 和相关的 IP 子网。随着托管主机的增加，这种分配给每个客户单一 VLAN 和 IP 子网的模型造成了巨大的扩展方面的局限。

为了解决上述问题，该 IDC 新购进了一台支持 PVLAN 的交换机 Cisco 3560，通过 PVLAN 机制将这些服务器划分到同一个 IP 子网中，但服务器只能与自己的默认网关通信。

※技术要领

(1)　PVLAN 的基本概念；
(2)　配置 PVLAN。

5.5.1　PVLAN 概述

随着网络的迅速发展，用户对于网络数据通信的安全性提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性。传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，每个客户从第 2 层被隔离开，可以防止任何恶意的行为和 Ethernet 的信息探听。然而，这种分配每个客户单一 VLAN 和 IP 子网的模型造成了巨大的可扩展方面的局限。这些局限主要有下述几方面。

✧　VLAN 的限制：交换机固有的 VLAN 数目的限制。
✧　复杂的 STP：对于每个 VLAN，每个相关的 Spanning Tree 的拓扑都需要管理。
✧　IP 地址的紧缺：IP 子网的划分势必造成一些 IP 地址的浪费。
✧　路由的限制：每个子网都需要相应的默认网关的配置。

从安全上考虑，现在有了一种新的 VLAN 机制，所有服务器在同一个子网中，但服务器只能与自己的默认网关通信，这一新的 VLAN 特性就是专用 VLAN(Private VLAN，PVLAN)。

1. PVLAN 的端口类型

在 PVLAN 的概念中，交换机端口有隔离端口(Isolated Port)、团体端口(Community Port)和混杂端口(Promiscuous Port)3 种类型。

✧ 隔离端口：这种类型的端口彼此之间不能交换数据，只能与混杂端口通信，一般用作用户的接入端口。
✧ 团体端口：这种类型的端口之间可以互相通信，也可以与混杂端口通信，主要应用在同一 PVLAN 中，给那些需要互相通信的一组用户使用。
✧ 混杂端口：这种类型的端口可以与同一 PVLAN 里面的所有端口互相通信，通常与路由器或第三层交换机相连接的端口都要配置成混杂端口，它收到的流量可以发往隔离端口和团体端口。

2. PVLAN 类型

PVLAN 有 3 种类型：主 VLAN(Primary VLAN)、隔离 VLAN(Isolated VLAN)和团体 VLAN(Community VLAN)。隔离端口属于隔离 VLAN(Isolated PVLAN)，团体端口属于团体 VLAN(Community VLAN)，而主 VLAN 代表一个 PVLAN 整体。

隔离 VLAN 和团体 VLAN 都属于辅助 VLAN(Secondary VLAN)，它们之间的区别是：同属于一个隔离 VLAN 的主机不可以互相通信，同属于一个团体 VLAN 的主机可以互相通信，但它们都可以和与之所关联的主 VLAN 通信。

PVLAN 的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需与自己的默认网关连接，一个 PVLAN 不需要多个 VLAN 和 IP 子网就提供了具备第二层数据通信安全性的连接，所有的用户都接入 PVLAN，从而实现了所有用户与默认网关的连接，而与 PVLAN 内的其他用户没有任何访问。PVLAN 功能可以保证同一个 VLAN 中的各个端口相互之间不能通信，但可以穿过 Trunk 端口。这样即使同一 VLAN 中的用户，相互之间也不会受到广播的影响。最近流行的 ARP 欺骗病毒，便可以通过这种方法进行隔离。例如，某个 VLAN 内发现 ARP 病毒后，将 VLAN 配置成为一个隔离 VLAN 后，ARP 广播报文仅会传向混杂端口，而不会广播到整个 VLAN 中。

5.5.2 配置 PVLAN

在配置 PVLAN 时，通常的原则如下。

✧ 把需要第 2 层隔离的主机放到同一个隔离 VLAN 或者不同的团体 VLAN 中。
✧ 把需要第 2 层通信的主机放到同一个团体 VLAN 中。
✧ 把公共的服务器或者上联端口放到主 VLAN 中(即将端口设置为混杂端口)。
✧ 网关可以是主 VLAN 上配一个 3 层地址或者在主 VLAN 上连一个路由器。
✧ 交换机的上联端口也可以是 Trunk，主 VLAN 和辅助 VLAN 都可以通过 Trunk 链路。

在很多 Cisco 低端交换机上仅支持隔离端口特性，在高端的 6500/4500 上可以支持完整的 PVLAN 属性。下面是 PVLAN 的配置过程。

❶ 如果需要交换机支持 PVLAN 机制，首先需要将交换机的 VTP 模式修改为透明模式。

```
Switch# vlan database
Switch(vlan)#vtp mode transparent
Switch(vlan)#exit
```

❷ 创建主 VLAN 和辅助 VLAN。

```
Switch(config)#vlan 900                          #创建主VLAN
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# vlan 901                    #创建隔离VLAN
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 902                    #创建团体VLAN
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#exit
```

❸ 在主 VLAN 中，关联辅助 VLAN。注意，一个主 VLAN 只可以关联一个隔离 VLAN 和多个团体 VLAN。

```
Switch(config)#vlan 900
Switch (config-vlan)#private-vlan association 901 , 902
```

❹ 如果要取消关联或者继续关联其他辅助 VLAN，可以使用如下命令。

```
Switch(config-vlan)#private-vlan association {add | remove} aux2-vlan
```

❺ 将需要隔离的端口加入隔离 VLAN 或团体 VLAN 中。

```
Switch(config)#interface vlan primary-vlan-id
Switch(config-if)#private-vlan mapping aux-vlan , aux1-vlan
Switch(config-if)#private-vlan mapping {add | remove} aux2-vlan
Switch(config)#interface GigabitEthernet 0/11      #将G0/11设置为隔离端口
Switch(config-if)# switchport
Switch(config-if)#switchport private-vlan host-association 900 901
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#interface GigabitEthernet 0/12   #将G0/12设置为团体端口
Switch(config-if)# switchport
Switch(config-if)# switchport private-vlan  host-association 900 902
Switch(config-if)# switchport mode private-vlan host
```

❻ 同时将交换机的上联端口、连接路由器端口、连接公共服务器端口的类型配置为混杂端口。

```
Switch(config)#interface GigabitEthernet 0/24
Switch(config-if)# switchport
Switch(config-if)# switchport private-vlan mapping 900 901,902
Switch(config-if)# switchport mode private-vlan promiscuous
```

❼ 保存配置和验证配置。

```
Switch(config-if)#end
Switch#copy run start
Switch#show interface Gi4/14 switchport
```

点评与拓展： 在配置 PVLAN 端口中，如果配置了 switchport access vlan xxx，这一句已经不起作用了，起作用的是 switchport private-vlan mapping xxx xxx,xxx。

5.6 防范其他常见 2 层攻击

5.6.1 防范 MAC 泛洪攻击

应用实例导航：Sadness 公司防范 MAC 泛洪攻击

※场景呈现

SC 最终因为多次攻击而被 Sadness 公司的安全部门发现，并将其解聘。SC 为了报复 Sadness 公司，又开始了新一轮的入侵。这次，SC 采用一个名为 Macof 的攻击软件，下面所示是攻击过程。

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S
1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S
446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S
105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S
1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S
1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S
1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S
727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S
605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S
2128143986:2128143986(0) win 512
```

不到 5 分钟，交换机的 CAM 表就被填满，开始广播数据，SC 继续开始监听网络中各种具有极大商业价值的机密。

※技术要领

(1) MAC 泛洪工作原理；

(2) 防范 MAC 泛洪攻击的配置方法。

交换机主动学习客户端的 MAC 地址，并建立和维护端口与 MAC 地址的对应表以建立交换路径，这个表就是通常我们所说的 CAM 表。CAM 表的大小是固定的，不同交换机的 CAM 表大小不同。

MAC/CAM 攻击就是利用工具(如 macof)发送大量带有随机源 MAC 地址的数据包，这些新 MAC 地址被交换机 CAM 学习，很快塞满 MAC 地址表，这时新目的 MAC 地址的数据包就会广播到交换机所有端口。当交换机的 CAM 表被填满，就开始利用广播方式传递数据，这时交换机就像共享 HUB 一样工作，黑客便可以用 sniffer 工具监听所有端口的流量。



此类攻击不仅造成安全性的破坏，同时大量的广播包也降低了交换机的性能。

采用交换机的端口安全和动态端口安全功能，可以限制单个端口所连接 MAC 地址的数目，有效防止类似 macof 工具和 SQL 蠕虫病毒发起的攻击。例如，交换机连接单台工作站的端口，可以限制所学 MAC 地址数为 1；连接 IP 电话和工作站的端口可限制所学 MAC 地址数为 3(分别用于 IP 电话、工作站和 IP 电话内的交换机)。

通过端口安全功能，还可以静态设置每个端口所允许连接的合法 MAC 地址，实现设备级的安全授权。动态端口安全功能则设置端口允许合法 MAC 地址的数目，并以一定时间内所学习到的地址作为合法 MAC 地址。

除上述两个功能之外，端口安全还可以设置超过规定 MAC 数量时的处理方法。

利用交换机的端口安全，防范 MAC 泛洪攻击的配置方法如下。

```
Switch(config)#switchport port-security
Switch(config)#switchport port-security maximum 3
Switch(config)#switchport port-security violation restrict
Switch(config)#switchport port-security aging time 2
Switch(config)#switchport port-security aging type inactivity
```

5.6.2 防范 DHCP 攻击

采用 DHCP 服务器可以自动为用户设置网络 IP 地址、子网掩码、默认网关、DNS 服务器、WINS 服务器等网络参数，简化了用户网络设置，提高了管理效率。但在 DHCP 管理和使用上也存在着一些令网管人员比较头痛的问题，主要如下。

- ✧ DHCP 服务器的冒充：网络用户有意或无意启动 DHCP 服务器功能，向其他用户发放错误的 IP 地址、DNS 服务器信息或默认网关信息；
- ✧ DHCP 服务器的 DoS 攻击：黑客利用类似 Goobler 的工具可以发出大量带有不同源 MAC 地址的 DHCP 请求，直到 DHCP 服务器对应网段的所有地址被占用；
- ✧ 用户随便指定地址，造成网络地址冲突。

为了能有效阻止上述攻击，我们可以在交换机上启用 DHCP Snooping(DHCP 侦听)功能。DHCP Snooping 是 DHCP 的安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息。通过截取一个虚拟局域网内的 DHCP 信息，交换机可以在用户与 DHCP 服务器之间担任小型安全防火墙的角色。

DHCP Snooping 功能基于动态地址分配建立了一个 DHCP 绑定表，并将该表存储在交换机里。在没有 DHCP 的环境中，绑定条目可能被静态定义。每个 DHCP 绑定条目包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息，用户可以如下命令查看该表。

```
Switch #show ip dhcp snooping binding
 MacAddress      IpAddress   Lease(sec)  Type      VLAN   Interface
 ------------------    ---------------    ----------    -------    ----
--------------------
00:0D:60:2D:45:0D   10.149.3.13     600735     dhcp-snooping        100
GigabitEthernet1/0/7
```

当交换机开启了 DHCP Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。

另外，DHCP Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址。默认情况下，所有用户端口都被认为不可信任端口，不应该作出任何 DHCP 响应，因此欺诈 DHCP 响应包被交换机阻断，合法的 DHCP 服务器端口或上联端口应被设置为信任端口。

在交换机中，配置 DHCP Snooping 的过程如下。

❶ 在全局模式配置，全局启用 DHCP 侦听功能。

```
Switch(config)#ip dhcp snooping
```

❷ 如果是针对某些 VLAN，还需要定义哪些 VLAN 启用 DHCP Snooping。

```
Switch(config)#ip dhcp snooping vlan 13,200
```

❸ 定义 DHCP 不信任端口，并设置 DHCP 包的转发速率，超过该速率时就关闭该端口(默认不限制)。

```
Switch(config-if)#no ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate 10
```

❹ 定义 DHCP 信任端口，使从该端口进入的 dhcpDHCP 服务器数据有效。

```
Switch(config-if)#ip dhcp snooping trust
```

5.6.3 防范 ARP 攻击

应用实例导航：Sadness 公司防范 ARP 攻击

※场景呈现

Sadness 公司网管在处理一起网络中断故障中，用户反映无法 Ping 通网关，但网关设备工作正常，他通过查询交换机发现，某个 MAC 在交换机内多次出现，并拥有多个不同的 IP。

```
Switch#show ip cache flow
Vl160      10.48.160.2     Null      10.48.160.255   11 0089 0089    3
Vl160      10.48.160.7     Null      10.48.160.255   11 0089 0089    3
Vl168      10.48.168.38    Null      10.48.168.255   11 008A 008A    1
Vl160      10.48.160.27    Null      10.48.160.255   11 0089 0089    9
Vl168      10.48.168.212   Null      10.48.168.255   11 008A 008A    1
Vl168      10.48.168.83    Null      10.48.168.255   11 0089 0089    9
Vl160      10.48.160.96    Null      10.48.160.255   11 0089 0089    1
Vl160      10.48.160.115   Null      10.48.160.255   11 0089 0089    6
Vl160      10.48.160.82    Null      10.48.160.255   11 0089 0089    1
Vl160      10.48.160.191   Null      10.48.160.255   11 008A 008A    1
Vl160      10.48.160.181   Null      10.48.160.255   11 008A 008A    1
Vl160      10.48.160.181   Null      10.48.160.255   11 0089 0089   12
Vl168      10.48.168.87    Null      10.48.163.231   06 0D8B 008B    1
Vl160      10.48.160.135   Null      10.48.160.255   11 0089 0089    3
```

后来该网管确认这样的攻击为 ARP 攻击，并查询了很多资料，最终使用 Cisco DAI 防止了这样的攻击再次产生。

在以太网中，数据帧从一个主机到达网内的另一台主机是根据 48 位的以太网地址(称为 MAC 地址)来确定接口的，而不是根据 32 位的 IP 地址。ARP(Address Resolution Protocol，地址解析协议)就是用于将计算机的 IP 地址映射成 MAC 地址的协议。正常情况下，同一网络中两台主机在第一次通信时，源主机首先以广播方式发送 ARP 请求(目的 MAC 设置为 FF-FF-FF- FF-FF-FF)，拥有此 IP 地址的目的主机将源主机 MAC 地址和 IP 地址的对应关系记录在 ARP 高速缓存，并予以 ARP 应答，返回自己的 IP 和 MAC 地址。源主机接收到 ARP 应答后，更新自己的 ARP 高速缓存。此后，源主机与目的主机就可以进行通信了。

ARP 同时支持一种无请求 ARP 功能，局域网段上的所有工作站都将收到主动 ARP 广播，将发送者的 MAC 地址和其宣布的 IP 地址保存在 ARP 高速缓存中。主动式 ARP 主要用来以备份的主机来替换失败的主机。由于 ARP 无任何身份校验机制，黑客利用程序发送误导的主动式 ARP，使网络流量都经过恶意攻击者的计算机，变成某个局域网段 IP 会话的中间人，从而达到窃取甚至篡改正常传输的目的。黑客程序发送的主动式 ARP 采用发送方私有 MAC 地址而非广播地址，通信接收方根本不会知道自己的 IP 地址被取代。为了保持 ARP 欺骗的持续有效，黑客程序每隔 30s 都会重发私有主动式 ARP。这就是 ARP 攻击。

ARP 攻击是现阶段出现频率最高的一种攻击行为，而且也是很多厂商网络设备比较难以防范的一种攻击行为。通常可以使用一些软件检测攻击行为，例如 AntiARP。图 5-9 所示的是 AntiARP 的使用界面。



图 5-9　AntiARP 界面

当然，用户可以通过 Windows 自带的 arp-a 命令查询网关 MAC 地址是否改变，或者使用 arp-s 静态绑定到网关的 IP 地址和 MAC 地址，防止受到 ARP 欺骗。

Cisco 交换机可以通过动态 ARP 检查(Dynamic ARP Inspection，DAI)来防止攻击。DAI 可以保证接入交换机只传递“合法”的 ARP 请求和应答信息。DHCP Snooping 监听绑定表，包括 IP 地址与 MAC 地址的绑定信息并将其与特定的交换机端口相关联，DAI 可以用来检查所有非信任端口的 ARP 请求和应答(主动式 ARP 和非主动式 ARP)，确保应答来自真正的 ARP 所有者。

交换机通过检查端口记录的DHCP 绑定信息和ARP 应答的IP 地址决定是否为真正的 ARP 所有者，不合法的 ARP 包将被删除。DAI 配置针对 VLAN，对于同一 VLAN 内的接口可以开启 DAI 也可以关闭。如果 ARP 包从一个可信任的接口接收到，就不需要做任何检查，如果 ARP 包从一个不可信任的接口上接收到，该包就只能在绑定信息被证明合法的

情况下才会被转发出去。这样，DHCP Snooping 对于 DAI 来说也成为必不可少的。DAI 是动态使用的，相连的客户端主机不需要进行任何设置上的改变。对于没有使用 DHCP 的服务器，个别机器可以采用静态添加 DHCP 绑定表或 ARP 访问控制列表实现。

另外，通过 DAI 可以控制某个端口的 ARP 请求报文频率。一旦 ARP 请求报文的频率超过预先设定的阈值，立即关闭该端口。该功能可以阻止网络扫描工具的使用，同时对有大量 ARP 报文特征的病毒或攻击也可以起到阻断作用。

DAI 通常是与 DHCP Snooping 一起使用的，配置方式如下。

❶ 在全局模式下，启用 DAI。

```
Switch(config)#ip dhcp snooping vlan 100,200 ,300,400
Switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping
Switch(config)#ip arp inspection vlan 100,200 ,300,400
Switch(config)#ip arp inspection log-buffer entries 1024
Switch(config)#ip arp inspection log-buffer logs 1024 interval 10
```

❷ 在接口模式下，对于不信任的端口做如下配置。

```
Switch(config-if)#no ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate 10
Switch(config-if)#no ip arp inspection trust
Switch(config-if)#ip arp inspection limit rate 15
```

❸ 在接口模式下，对于信任的端口做如下配置。

```
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip arp inspection trust
```

❹ 对于没有如上功能的交换机可以采用静态绑定的方式。

```
Switch(config)#arp access-list static-arp
Switch(config)#permit ip host 10.0.3.3 mac host 000a.ebac.3312
Switch(config)#ip arp inspection filter static-arp vlan 200
```

❺ 用户可以查看日志，可以看到攻击主机被拒绝。

```
 Switch#show log:
4w6d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 296 milliseconds
on Gi3/2.
4w6d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/2, putting Gi3/2
in err-disable state
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.2/12:19:27  UTC
Wed Apr 19 2000])
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.3/12:19:27  UTC
Wed Apr 19 2000])
```

📖点评与拓展：针对网络第二层的攻击是最容易实施也是最不容易被发现的安全威胁，它可以使网络瘫痪或者通过非法获取密码等敏感信息的方式来危及网络用户的安全。由于任何一个合法用户都能获取一个以太网端口的访问权限，而这些用户都有可能成为黑客；同时，由于设计 OSI 模型的时候，允许不同通信层处于相对独立的工作模式，因此承载所有客户关键应用的网络第二层的安全就变得至关重要。

5.7 本章小结

这一章通过交换式网络攻击行为的案例，详细介绍了 STP、VTP、VLAN 以及动态 VLAN 和私有 VLAN 等交换网络中常见的配置方式。然后通过对一些常见攻击方式的分析，讲述了 MAC 泛洪、DHCP 攻击以及 ARP 欺骗等较为常见的攻击手法以及防范手段。下一章我们将介绍关于网络安全接入准则以及系统升级的方法以使网络更加安全。

第 6 章　网络身份认证服务

在网络安全中讨论得最多的问题在于如何识别真正的用户，以及如何使用有效的身份认证方式等。目前网络的安全认证包括两个方面：一个来自基于 RADIUS(远程认证拨入用户服务协议)认证的 VPN(虚拟专用网络)远程接入、802.1x 局域网接入以及无线网接入等认证；另一方面则来自数据在网络传输过程中所采用的电子证书服务。

通过本章的学习，读者应掌握以下主要内容：

✧　PKI 证书体系
✧　Windows 电子证书服务
✧　AAA 认证授权统计
✧　RADIUS 认证服务

6.1　电子证书服务

6.1.1　PKI 公钥基础结构

PKI(Public Key Infrastructure，公钥基础设施)是一个用非对称密码算法原理和技术实现的、具有通用性的安全基础设施。PKI 利用数字证书标识密钥持有人的身份，通过对密钥的规范化管理，为组织机构建立和维护一个可信赖的系统环境，透明地为应用系统提供身份认证、数据保密性和完整性、不可否认性等各种必要的安全保障，满足各种应用系统的安全需求。简单的说，PKI 是提供公钥加密和数字签名服务的系统，目的是为了自动管理密钥和证书，保证网上数字信息传输的机密性、真实性、完整性和不可否认性。

1. 需要 PKI 的原因

随着网络技术的发展，特别是 Internet 的全球化，各种基于互联网技术的网上应用，如电子政务、电子商务等得到了迅猛发展。网络正逐步成为人们工作、生活中不可分割的一部分。由于互联网的开放性和通用性，网上的所有信息对所有人都是公开的，因此应用系统对信息的安全性提出了更高的要求。

1)　对身份合法性验证的要求

以明文方式存储、传送的用户名和口令存在着被截获、破译等诸多安全隐患；同时，还有维护不便的缺点。因此，需要一套安全、可靠并易于维护的用户身份管理和合法性验证机制来确保应用系统的安全性。

2)　对数据保密性和完整性的要求

企业应用系统中的数据一般都是明文，在基于网络技术的系统中，这种明文数据很容

易泄密或被篡改，必须采取有效的措施保证数据的保密性和完整性。

3) 对传输安全性的要求

以明文方式在网上传输的数据，很容易被截获导致泄密，因此必须对通信通道进行加密保护。利用通信专线的传统方式已经远远不能满足现代网络应用发展的需求，必须寻求一种新的方法来保证基于互联网技术的传输安全需求。

4) 对数字签名和不可否认的要求

不可否认性为了防止事件发起者事后抵赖，对于规范业务，避免法律纠纷起着很大的作用。传统不可否认性是通过手工签名完成的，在网络应用中需要一种具有同样功能的机制来保证不可否认性，那就是数字签名技术。

PKI 基于非对称公钥体制，采用数字证书管理机制，可以为透明地为网上应用提供上述各种安全服务，极大地保证了网上应用的安全性。

2. PKI 的功能组成结构

PKI(公钥基础设施)体系主要由 KMC(密钥管理中心)、CA(认证机构)、RA(注册审核机构)、证书/CRL 发布系统和应用接口系统五部分组成。

- ✧ 密钥管理中心(KMC)：密钥管理中心向 CA 服务提供相关密钥服务，如密钥生成、密钥存储、密钥备份、密钥恢复、密钥托管和密钥运算等。
- ✧ CA(认证机构)：认证机构是 PKI 公钥基础设施的核心，它主要完成生成/签发证书、生成/签发证书撤销列表(CRL)、发布证书和 CRL 到目录服务器、维护证书数据库和审计日志库等功能。
- ✧ RA(注册审核机构)：RA 是数字证书的申请、审核和注册中心。它是 CA(认证机构)的延伸。在逻辑上 RA 和 CA 是一个整体，主要负责提供证书注册、审核以及发证功能。
- ✧ 证书/CRL 发布系统：该发布系统主要提供 LDAP(转型目录访问协议)服务、OCSP(联机证书状态协议)服务和注册服务。注册服务为用户提供在线注册的功能；LDAP 服务提供证书和 CRL 的目录浏览服务；OCSP 服务提供证书状态在线查询服务。
- ✧ 应用接口系统：应用接口系统为外界提供使用 PKI 安全服务的入口。应用接口系统一般采用 API、JavaBean、COM 等多种形式。一个典型、完整、有效的 PKI 应用接口系统至少应具有以下部分。
  - 公钥密码证书管理(证书库)；
  - 黑名单的发布和管理(证书撤销)；
  - 密钥的备份和恢复；
  - 自动更新密钥；
  - 自动管理历史密钥。

3. PKI 的应用模式

PKI 提供的安全服务恰好能满足电子商务、电子政务、网上银行、网上证券等金融业交易的安全需求，是确保这些活动顺利进行必备的安全措施。没有这些安全服务，电子商务、电子政务、网上银行、网上证券等都无法正常运作。

1)　电子商务

电子商务的参与方一般包括买方、卖方、银行和作为中介的电子交易市场。当买方登录服务器时，互相需要验证对方的证书以确认其身份，这被称为双向认证。

在双方身份被互相确认以后，建立起安全通道并进行讨价还价，之后向商场提交订单。订单里有两种信息：一部分是订货信息，包括商品名称和价格；另一部分是提交银行的支付信息，包括金额和支付账号。买方对这两种信息进行“双重数字签名”，分别用商场和银行的证书公钥加密上述信息。当商场收到这些交易信息后，留下订单信息，而将支付信息转发给银行。商场只能用自己专有的私钥解开加密的订单信息并验证签名。同理，银行只能用自己的私钥解开加密的支付信息，验证签名并进行划账。银行在完成划账以后，通知起中介作用的电子交易市场、物流中心和买方，并进行商品配送。整个交易过程都是在 PKI 所提供的安全服务之下进行，实现了安全、可靠、保密和不可否认性。

2)　电子政务

电子政务包含的主要内容有：网上信息发布、办公自动化、网上办公、信息资源共享等。按应用模式也可分为 G2C、G2B、G2G，PKI 在其中的应用主要是解决身份认证、数据完整性、数据保密性和不可抵赖性等问题。

例如，一个保密文件发给谁或者哪一级公务员有权查阅某个保密文件等，这些都需要进行身份认证，与身份认证相关的还有访问控制，即权限控制。认证通过证书进行，而访问控制通过属性证书或访问控制列表(ACL)完成。有些文件在网络传输中要加密以保证数据的保密性；有些文件在网上传输时要求不能被丢失和篡改；特别是一些保密文件的收发必须要有数字签名等。只有 PKI 提供的安全服务才能满足电子政务中的这些安全需求。

3)　网上银行

网上银行是指银行借助互联网技术向客户提供信息服务和金融交易服务。银行通过互联网向客户提供信息查询、对账、网上支付、资金划转、信贷业务、投资理财等金融服务。网上银行的应用模式有 B2C 个人业务和 B2B 对公业务两种。

网上银行的交易方式是点对点的，即客户对银行。客户浏览器端装有客户证书，银行服务器端装有服务器证书。当客户上网访问银行服务器时，银行端首先要验证客户端证书，检查客户的真实身份，确认是否为银行的真实客户；同时银行服务器还要到 CA 的目录服务器，通过 LDAP 协议查询该客户证书的有效期和是否进入“黑名单”；认证通过后，客户端还要验证银行服务器端的证书。双向认证通过以后，建立起安全通道，客户端提交交易信息，经过客户的数字签名并加密后传送到银行服务器，由银行后台信息系统进行划账，并将结果进行数字签名返回给客户端。这样就做到了支付信息的保密和完整以及交易双方的不可否认性。

4)　网上证券

网上证券广义地讲是证券业的电子商务，它包括网上证券信息服务、网上股票交易和网上银证转账等。一般来说，在网上证券应用中，股民为客户端，装有个人证书；券商服务器端装有 Web 证书。在线交易时，券商服务器只需要认证股民证书，验证是否为合法股民，是单向认证过程，认证通过后，建立起安全通道。股民在网上的交易提交同样要进行数字签名，网上信息要加密传输；券商服务器收到交易请求并解密，进行资金划账并做数字签名，将结果返回给客户端。

6.1.2 安装证书服务

证书服务是 Windows Server 2003 操作系统的核心组件之一。根据需要，可以将 Windows Server 2003 配置成企业根 CA、企业从属 CA、独立根 CA 或独立从属 CA。本节将介绍企业根 CA 的配置过程。

1. 配置活动目录服务

企业根 CA 需要活动目录服务(Active Directory，AD)支持。AD 的配置方法如下。

❶ 依次单击【开始】→【运行】菜单，在打开的【运行】对话框中输入 dcpromo 命令，单击【确认】按钮，如图 6-1 所示。



图 6-1 安装 AD

❷ 弹出【Active Directory 安装向导】对话框，单击【下一步】按钮，如图 6-2 所示。



图 6-2 AD 安装向导

❸ 系统会自动产生一个兼容性提示，单击【下一步】按钮，如图 6-3 所示。

❹ 在【域控制器类型】向导页中，选中【新域的域控制器】单选按钮，并单击【下一步】按钮，如图 6-4 所示。

❺ 在【新的域名】向导页中，输入新域的 DNS 的名称，并单击【下一步】按钮，如图 6-5 所示。

❻ 以后的向导页均可选择默认值，直接单击【下一步】按钮即可。由于 AD 服务需要 DNS 支持，因此如果 DNS 服务尚未安装，它会检测一个错误并提示。选中【在这台计算机上安装

并配置 DNS 服务器，并将这台 DNS 服务器设为这台计算机的首选 DNS 服务器】单选按钮，如图 6-6 所示。

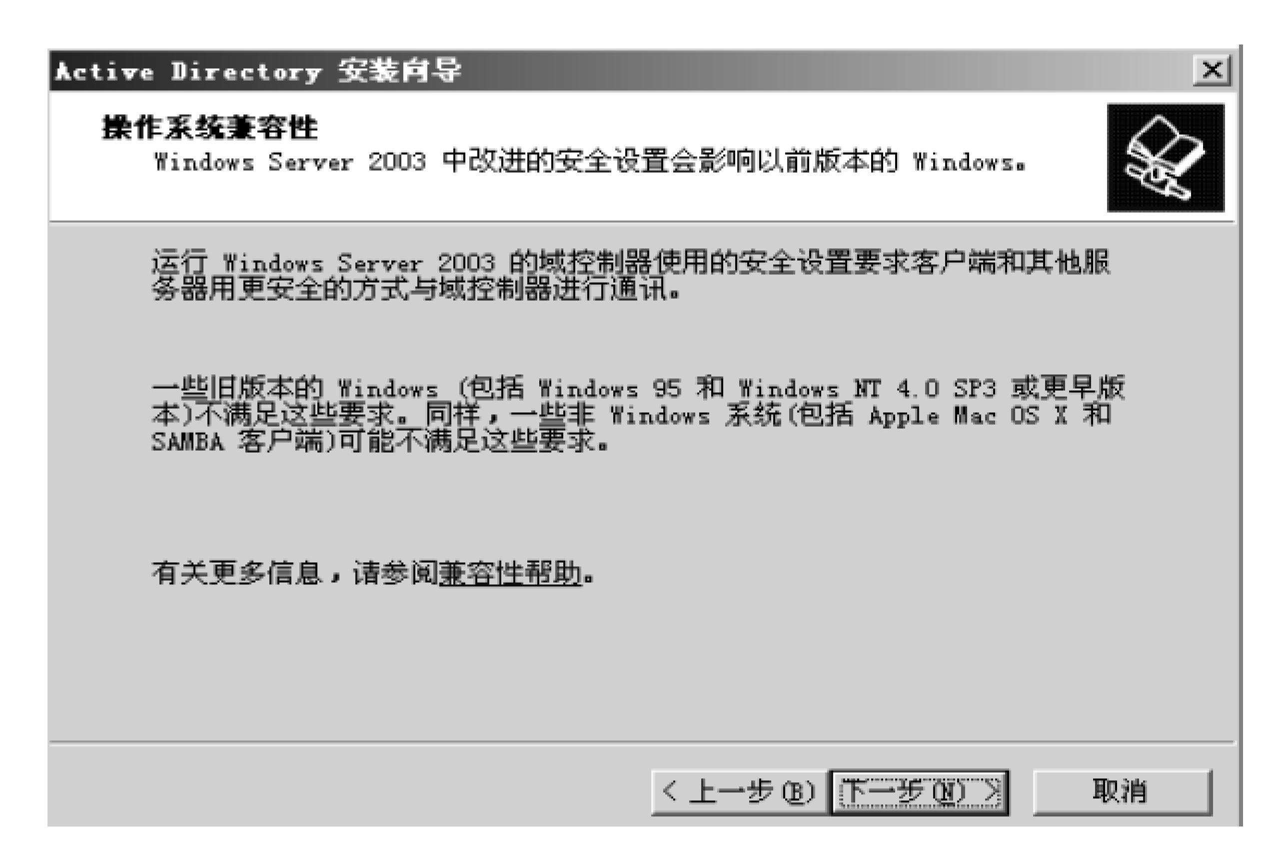


图 6-3　安装 AD 兼容性提示

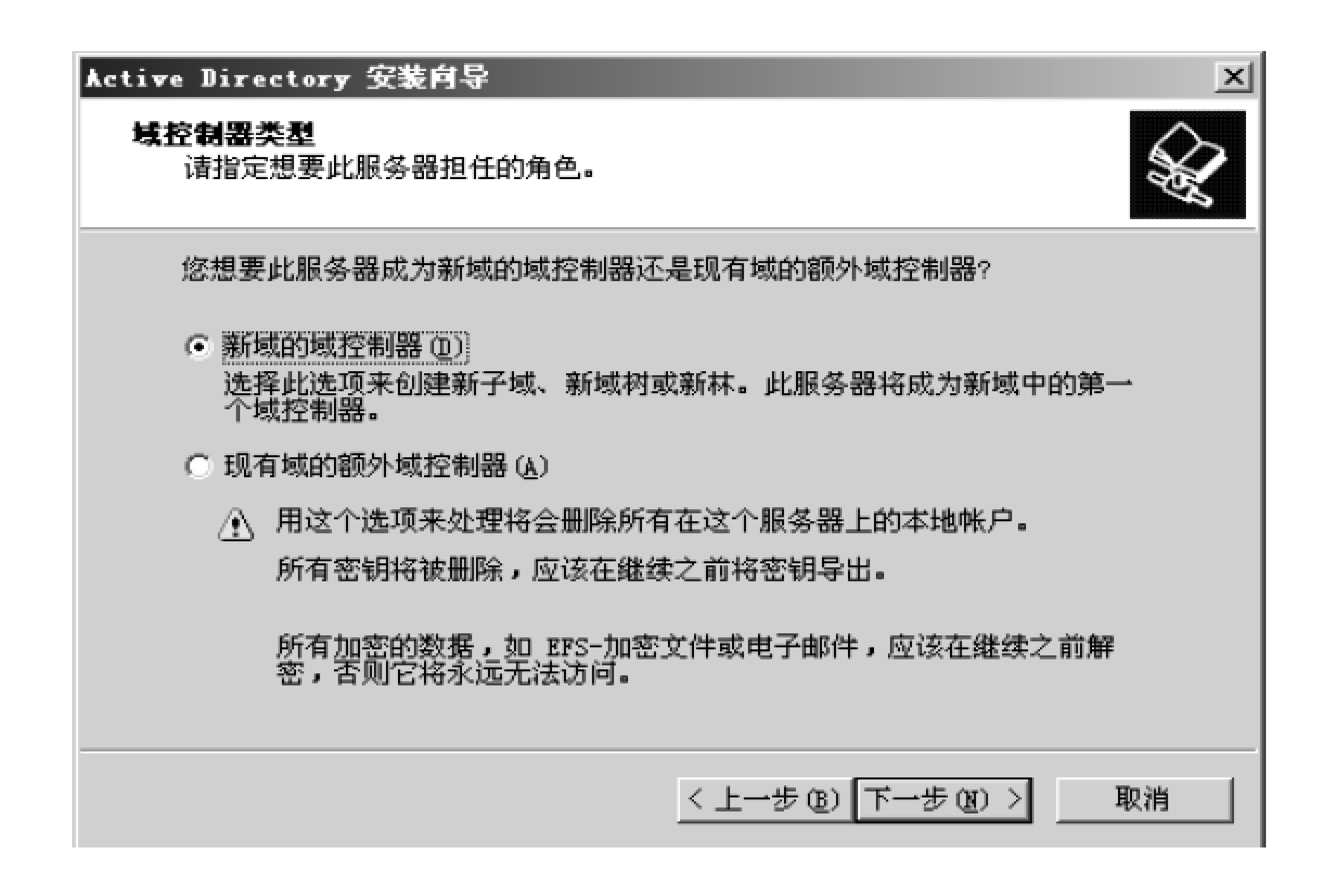


图 6-4　选择域控制器类型



图 6-5　输入 Active Directory 的 DNS 名称

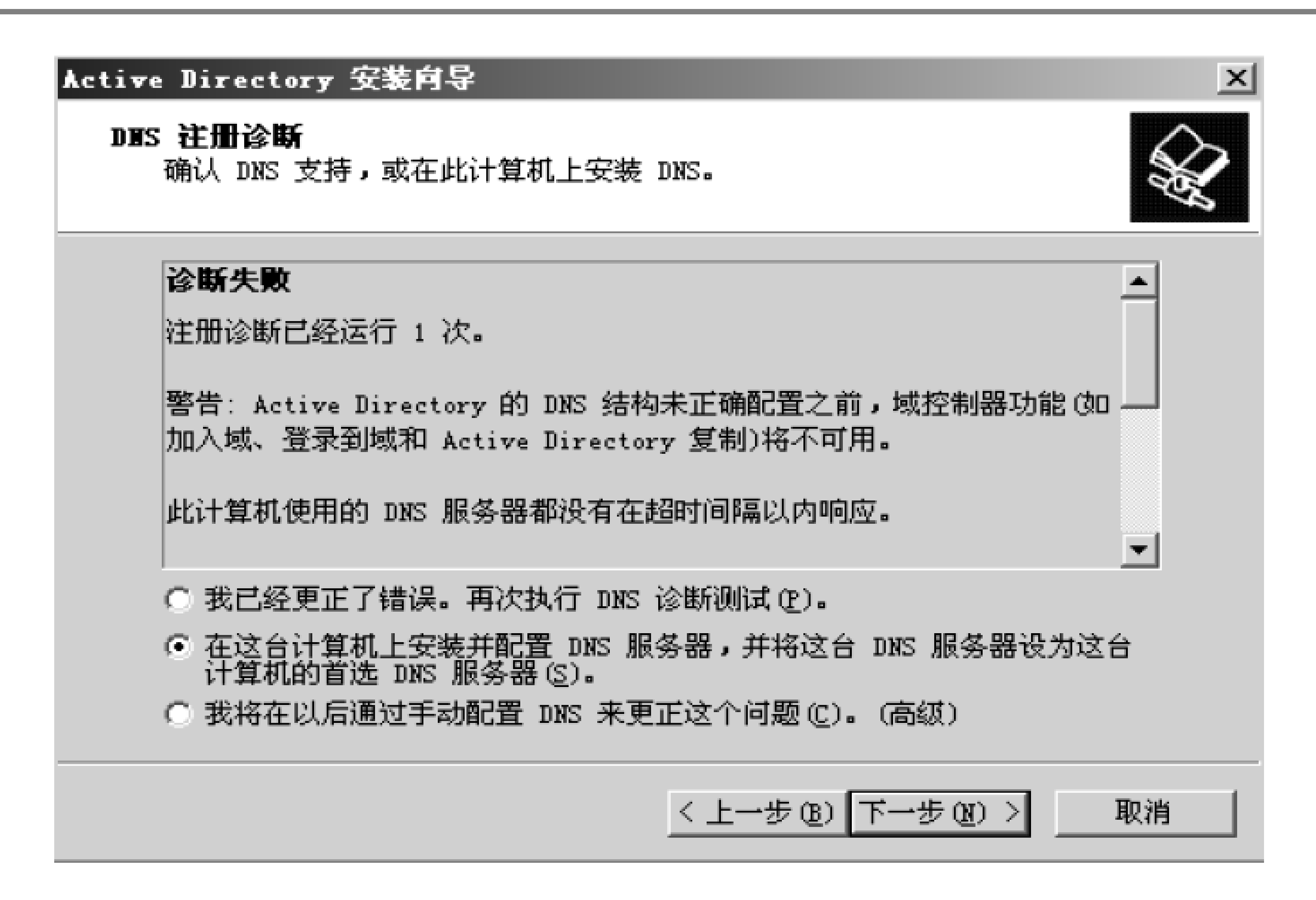


图 6-6　提示安装 DNS

❼ 在【权限】向导页，选中【只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限】单选按钮，单击【下一步】按钮，并在下一页中输入密码，如图 6-7 所示。

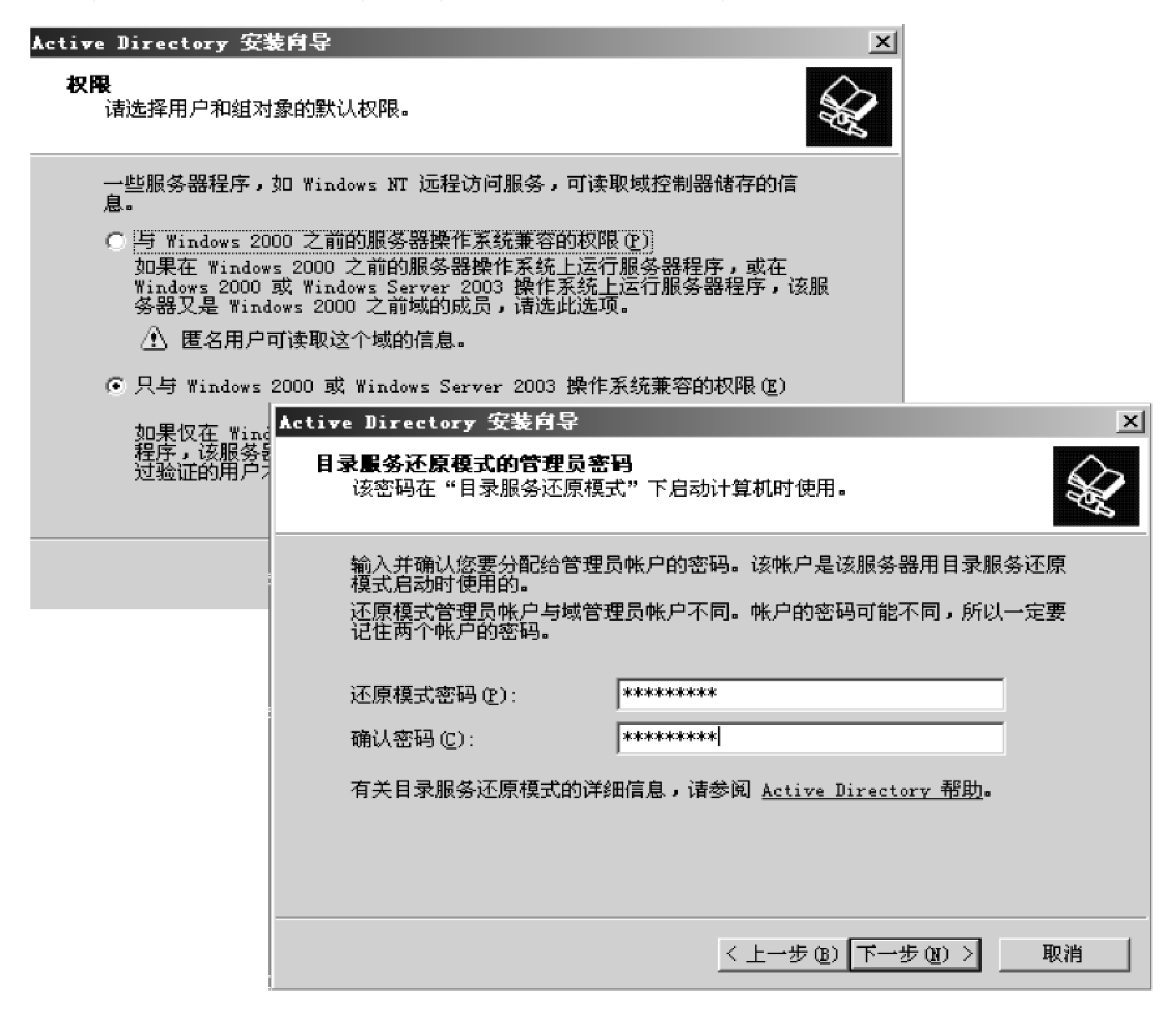


图 6-7　权限分配

❽ 此后系统会自动安装 AD，如图 6-8 所示。完成后重新启动计算机即可使用，完成 AD 安装后如图 6-9 所示。



图 6-8　安装 AD



图 6-9　完成 AD 安装

2. 配置证书服务

完成 AD 安装后，就可以进行证书服务的配置了，其配置方法如下。

❶ 依次单击【开始】→【控制面板】→【添加或删除程序】菜单，在打开的【添加或删除程序】窗口中，单击【添加/删除 Windows 组件】图标，如图 6-10 所示。



图 6-10　【添加或删除程序】窗口

❷ 在【Windows 组件向导】对话框中，在【组件】列表框中选中【证书服务】复选框，如图 6-11 所示。

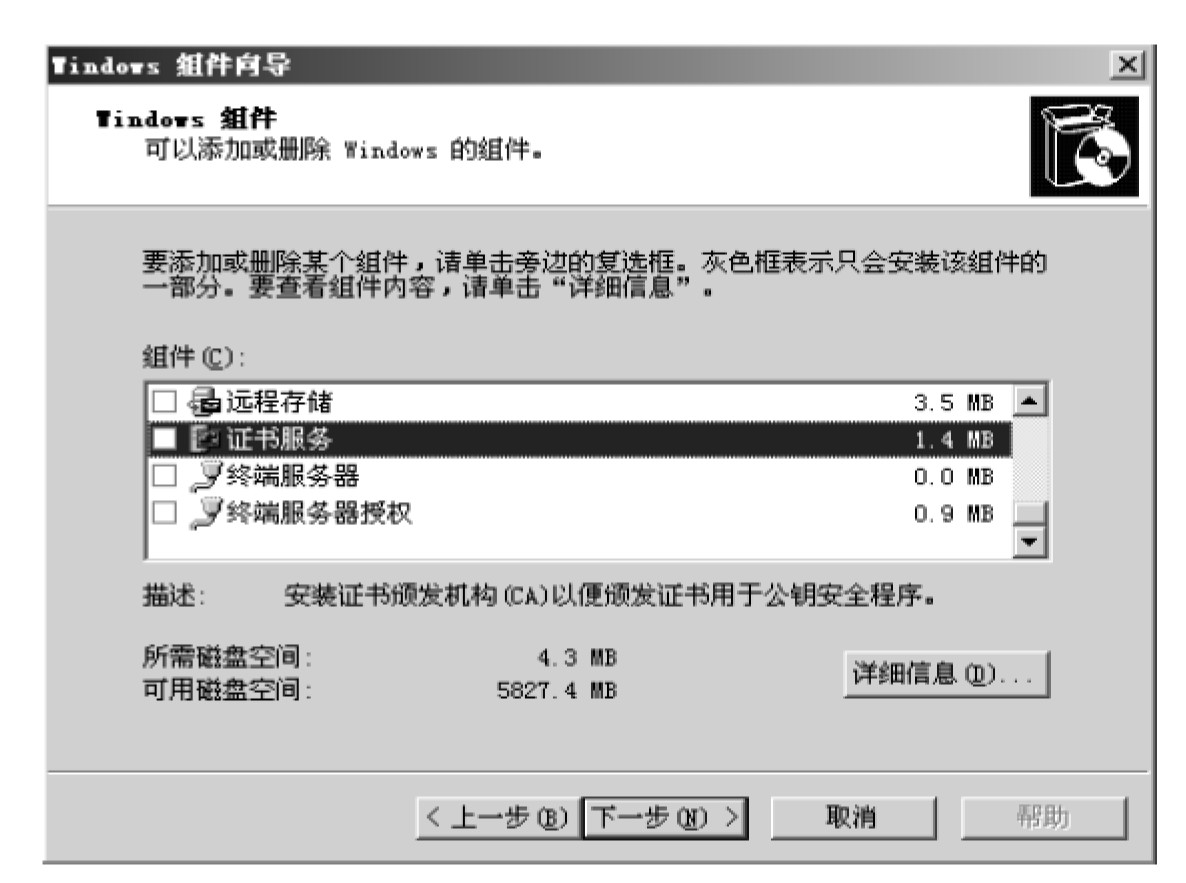


图 6-11 【Windows 组件向导】对话框

❸ 弹出【Windwos 证书服务】警告提示框，提示用户安装证书服务后，将无法再重命名服务器，并无法加入域或者删除域，确认后单击【是】按钮，如图 6-12 所示。

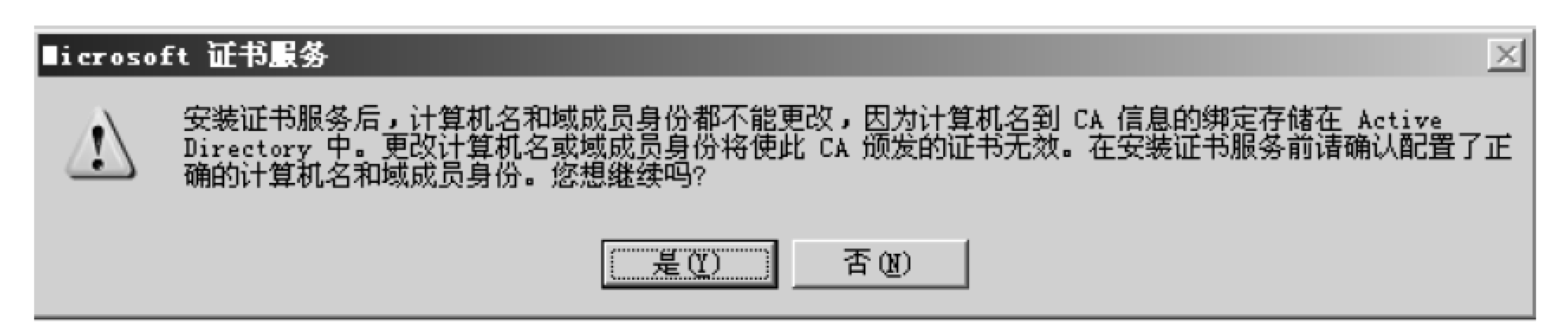


图 6-12 【Windows 证书服务】警告提示框

❹ 在【CA 类型】向导页中，设置 CA 类型。通常很多企业仅有单个域，因此这里选中【企业根 CA】单选按钮，并单击【下一步】按钮，如图 6-13 所示。

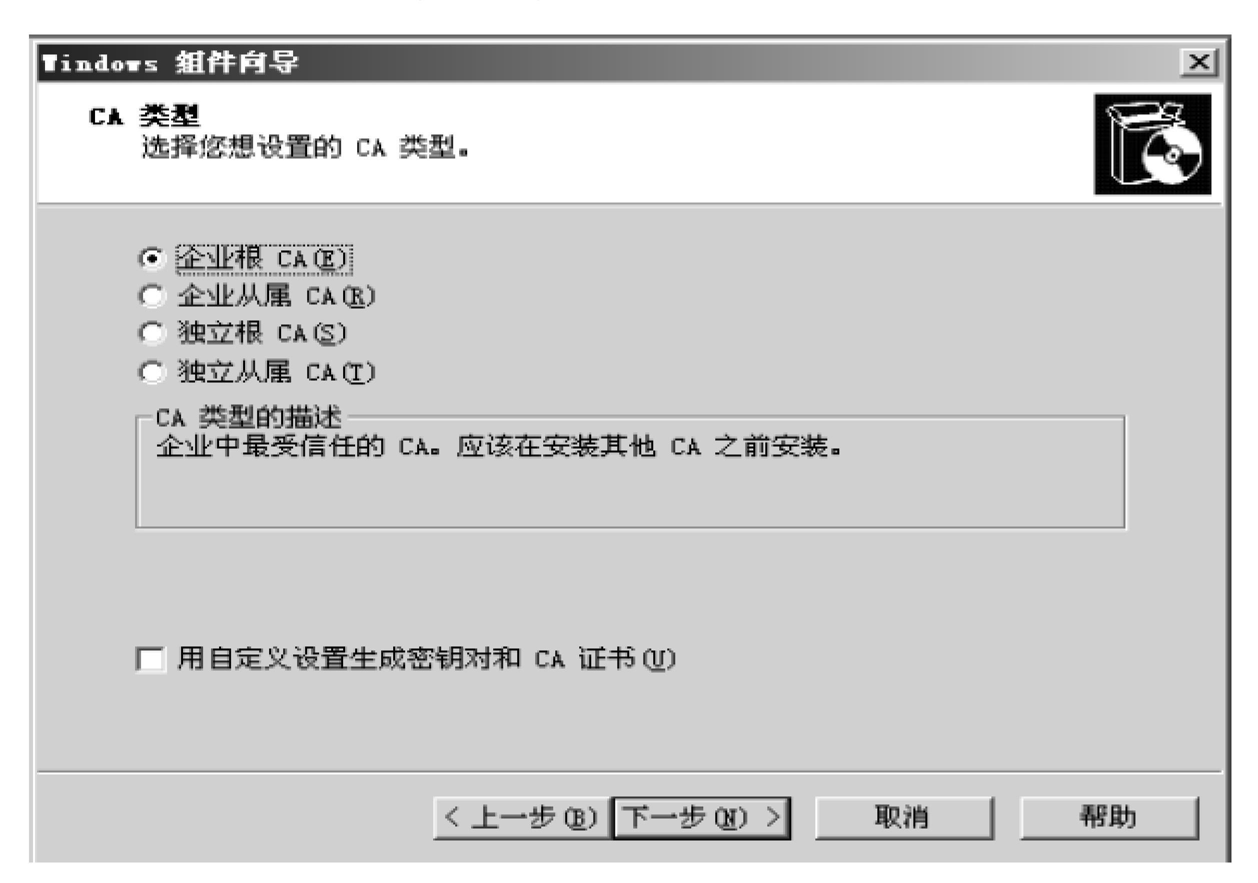


图 6-13 选择 CA 类型

❺ 在【CA 识别信息】向导页中，配置 CA 的公用名称和证书有效期限，并单击【下一步】按

钮，如图 6-14 所示。



图 6-14　配置 CA 识别信息

❻ 在【证书数据库设置】向导页中，设置证书数据库、证书数据库日志和配置信息的存储位置，设置完毕后单击【下一步】按钮，如图 6-15 所示。



图 6-15　设置证书数据库

❼ Windows 将自动进行安装，安装过程中，如果没有启动 IIS(因特网信息服务系统)，系统将告知无法使用 Web 注册功能。如果安装了 IIS，将警告系统会暂时关闭 IIS。单击【确定】按钮继续安装，这样就完成了证书服务的安装。

6.1.3 用户申请证书

申请和接收证书的方式取决于颁发该证书的证书颁发机构(CA)所使用的策略和过程。例如，某些 CA 可以提交申请网页，或者完成 AD 和证书服务的计算机成为域用户后，并授予了申请证书权限，则可以使用证书管理单元申请证书。

1. 证书模板

使用证书模板可以定义 Windows 2000 Enterprise CA 颁发的证书种类。任意访问控制列表(DACL)都与证书模板相关联，定义哪些安全主体拥有读取、注册和配置证书模板的权限。Enterprise CA 集成于 Active Directory 中。在 Active Directory(在整个目录林中有效)中可以定义证书模板和模板对象的 DACL。如果有多个 Enterprise CA 在 Windows 目录林中运行，权限的改变将影响所有 Enterprise CA。

Windows 2000 企业版 CA 使用的证书模板称为版本 1 证书模板。Windows 2000 附带了大量预定义的版本 1 证书模板，但是并不允许修改这些默认的证书模板。唯一可以进行的修改是权限，以允许注册证书模板。安装 Enterprise CA 后，在默认情况下将创建版本 1 证书模板。

Windows Server 2003 通过引入版本 2 模板扩展证书模板。版本 2 模板允许在该模板中自定义大多数设置。默认配置提供多个预配置的版本 2 模板，并允许根据需要添加更多的模板，这为管理员提供了完全的配置灵活性；或者，可以复制版本 1 证书模板，生成能够分别进行修改和保护的版本 2 证书模板。

注意： 与 Windows 2000 相似，Windows Server 2003 标准版仅支持版本 1 模板。Windows Server 2003 企业版和 Windows Server 2003 数据中心版对版本 1 和版本 2 模板都支持。基于版本 2 模板的证书仅能由运行 Windows Server 2003 企业版或 Windows Server 2003 数据中心版的 Enterprise CA 颁发。

在定义证书模板时，证书模板的定义必须对目录林中的所有 CA 可用。这通过将证书模板信息存储在配置名称上下文(CN=Configuration，DC=ForestRootName)来实现。该信息的复制取决于 Active Directory 的复制安排，而且在复制完成之前证书模板对所有 CA 都不可用。该存储和复制由 Windows Server 2003 系列计算机自动完成。表 6-1 是 Windows 2003 预配置的证书模板。

表 6-1　Windows 2003 预配置的证书模板

名 称	描　述	密钥用途	接收方类型	向 AD 发布
管理员	允许信任列表签名和用户身份验证	签名和加密	用户	是
已验证身份的会话	接受方能够通过 Web 服务器验证身份	签名	用户	否
Basic EFS	加密文件系统 (EFS) 用其对数据进行加密	加密	用户	是
CA 交换	用于存储为私钥存档配置的密钥	加密	计算机	否

续表

名 称	描 述	密钥用途	接收方类型	向 AD 发布
CEP 加密	允许所有者充当注册颁发机构 (RA)，以满足简单证书注册协议 (SCEP) 的要求	加密	计算机	否
代码签名	用于以数字方式签名的软件	签名	用户	否
计算机身份验证	允许计算机通过网络对自身进行身份验证	签名和加密	计算机	否
交叉证书颁发机构	在交叉证书和限定的下一级别中使用	签名	CrossCA	是
目录电子邮件复制	用于复制 Active Directory 中的电子邮件	签名和加密	DirEmailRep	是
域控制器	域控制器拥有的各种用途的证书	签名和加密	DirEmailRep	是
域控制器身份验证	用于验证 Active Directory 计算机和用户的身份	签名和加密	计算机	否
EFS 恢复代理	允许接收方对先前使用 EFS 进行加密的文件进行解密	加密	用户	否
注册代理	用于代表另一个接收方请求证书	签名	用户	否
注册代理(计算机)	用于代表另一个计算机接收方请求证书	签名	计算机	否
交换注册代理(脱机请求)	用于代表另一个接收方请求证书，并在请求中提供接收方名称	签名	用户	否
仅交换签名	用于 Microsoft 交换密钥管理服务，向 Exchange 用户颁发证书，使用户能够以数字方式对电子邮件进行签名	签名	用户	否
交换用户	用于 Microsoft 交换密钥管理服务，向 Exchange 用户颁发证书，对电子邮件进行加密	加密	用户	是
IPSEC	用于 IP 安全 (IPSec)，对网络通信进行数字签名、加密和解密	签名和加密	计算机	否
IPSEC(脱机请求)	用于 IP 安全 (IPSec)，对网络通信进行数字签名、加密和解密(当在要求中提供接收方名称时)	签名和加密	计算机	否
密钥恢复代理	该证书可以恢复在证书颁发机构存档的私钥	加密	KRA	是
根证书颁发机构	用于验证根证书颁发机构的身份	签名	CA	是

续表

名 称	描 述	密钥用途	接收方类型	向 AD 发布
智能卡登录	允许所有者使用智能卡进行身份验证	签名和加密	用户	否
智能卡用户	允许所有者使用智能卡对电子邮件进行身份验证和保护	签名和加密	用户	是
从属证书颁发机构	用于证明根证书颁发机构(由父或根证书颁发机构颁发)的身份	签名	CA	是
信任列表签名	所有者能够以数字方式对信任列表进行签名	签名	用户	否
用户身份验证	用户用于电子邮件、EFS 和客户端身份验证的证书	签名和加密	用户	是
仅用户签名	允许用户以数字方式对数据进行签名	签名	用户	否
Web 服务器	验证 Web 服务器的身份	签名和加密	计算机	否
路由器 (脱机请求)	用于通过 SCEP 从持有 CEP 加密证书的 CA 请求的路由器	签名和加密	计算机	否

2. 证书申请

申请证书前，我们需要配置用户对证书模板的使用权限，在【Active Directory 站点服务】管理单元中列出了当前系统的所有证书模板，它们拥有不同的用户权限，因此我们需要按照自己的需求来配置这些权限。

证书模板权限设置的步骤如下。

❶ 依次单击【开始】→【程序】→【管理工具】→【Active directory 站点与服务】菜单，打开【Active directory 站点和服务】窗口，如图 6-16 所示。

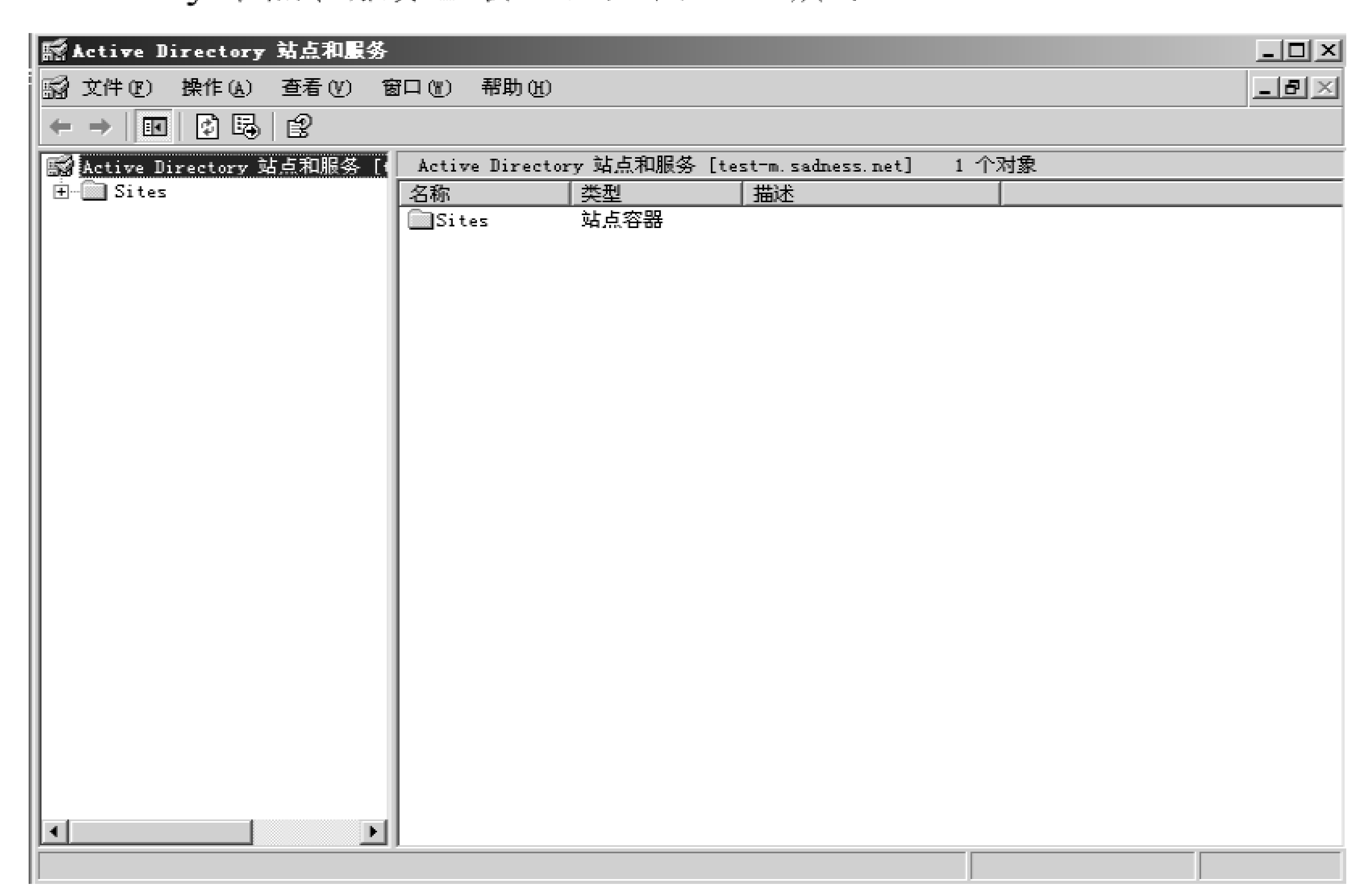


图 6-16 【Active Directory 站点和服务】窗口

❷ 选择左侧窗格中的【Active Directory 站点和服务】图标，选择【查看】→【显示服务器结点】命令，展开控制台树，然后在 Public Key Services 结点下选择 Certificate Templates 选项，右边就会列出所有证书模板，如图 6-17 所示。

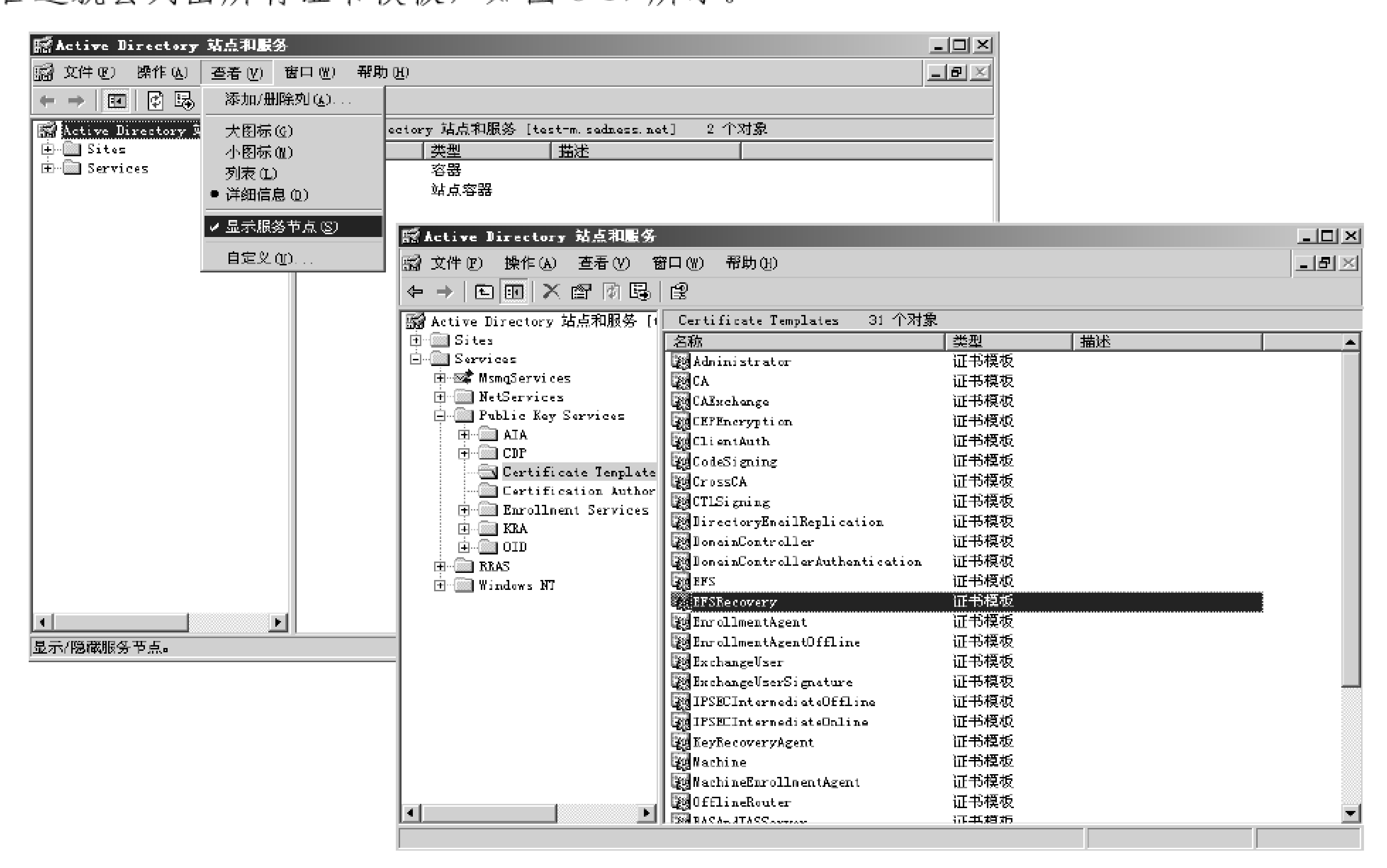


图 6-17　显示证书模板

❸ 配置用户对模板的使用权限。对于不同的模板，系统有不同的默认权限。当然，系统默认所有用户都可以使用 User 证书模板。而对于如域控制器等，则拥有不同的权限，管理员可以按照需要修改这些权限，如图 6-18 所示。

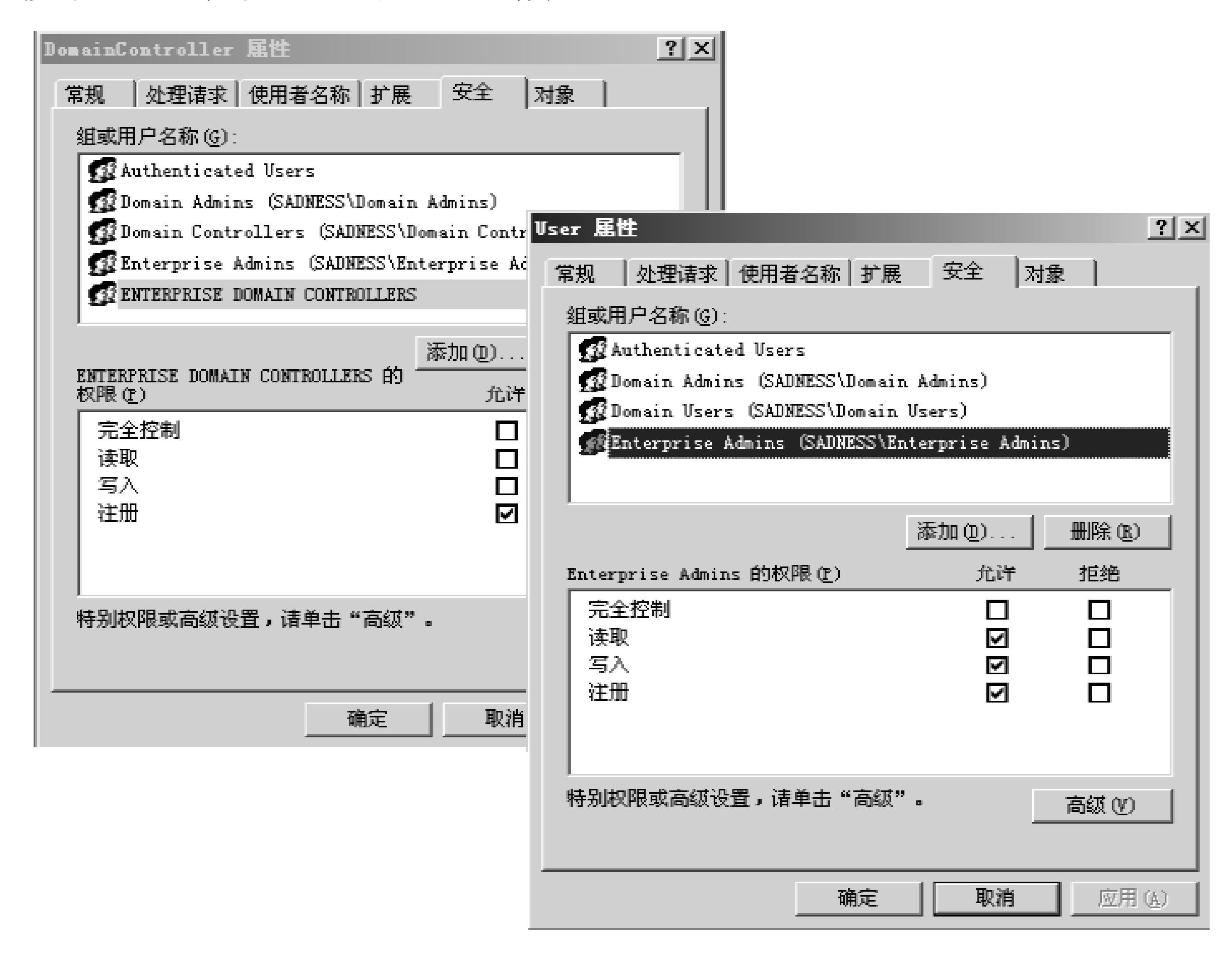


图 6-18　证书模板权限

❹ 依次单击【开始】→【运行】菜单，在【运行】对话框中输入 mmc 命令，进入【控制台】窗口，然后单击【文件】→【添加/删除管理单元】命令，如图 6-19 所示，打开【添加/删除管理单元】对话框。



图 6-19　控制台窗口

❺ 单击【添加】按钮，在【添加独立管理单元】对话框中选择【证书】选项，然后依次单击【完成】和【关闭】按钮，如图 6-20 所示。

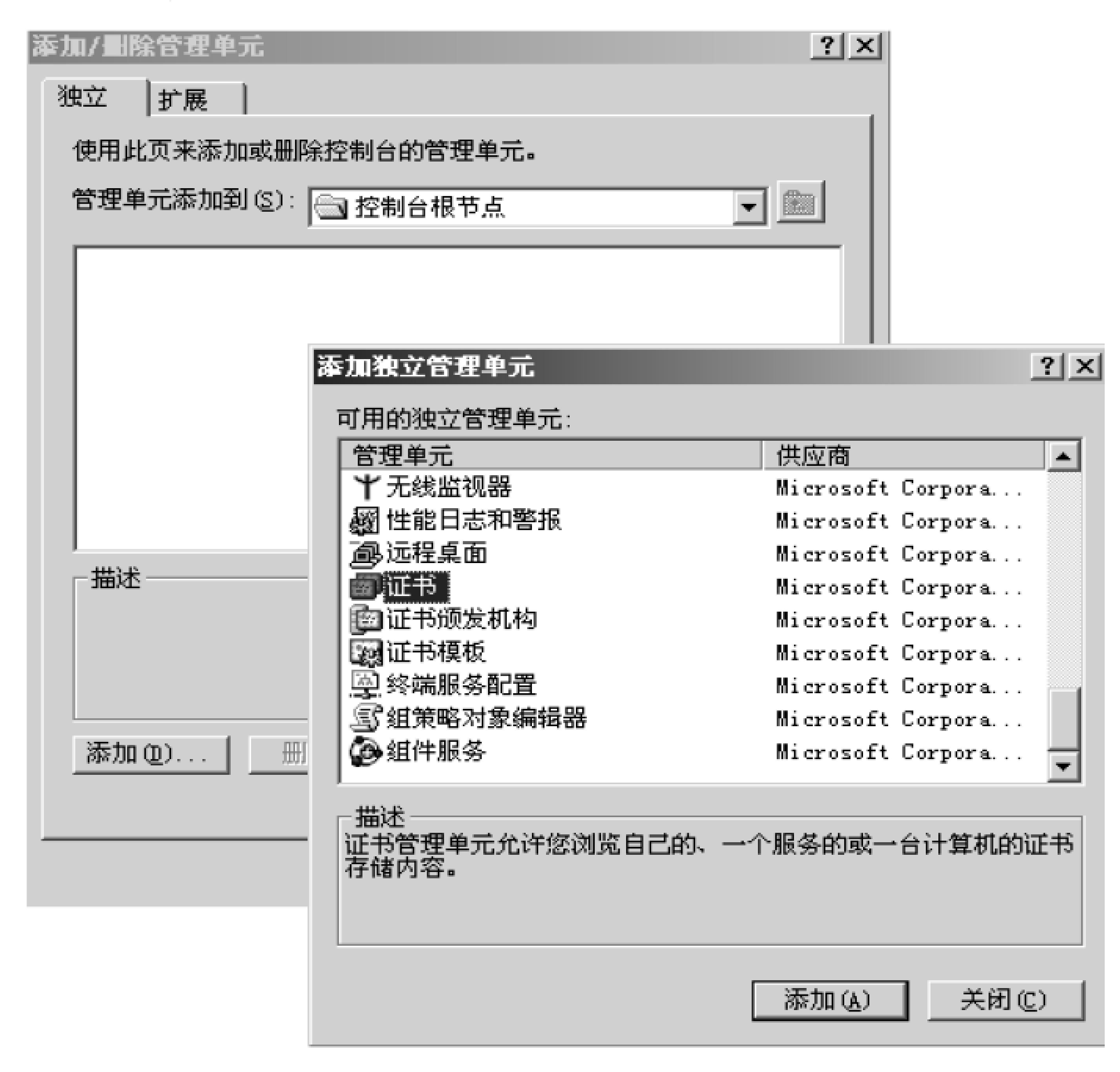


图 6-20　添加证书并进入管理控制台

❻ 在【证书管理单元】对话框中选中【我的用户帐户】单选按钮，然后依次单击【完成】和【关闭】按钮，如图 6-21 所示。

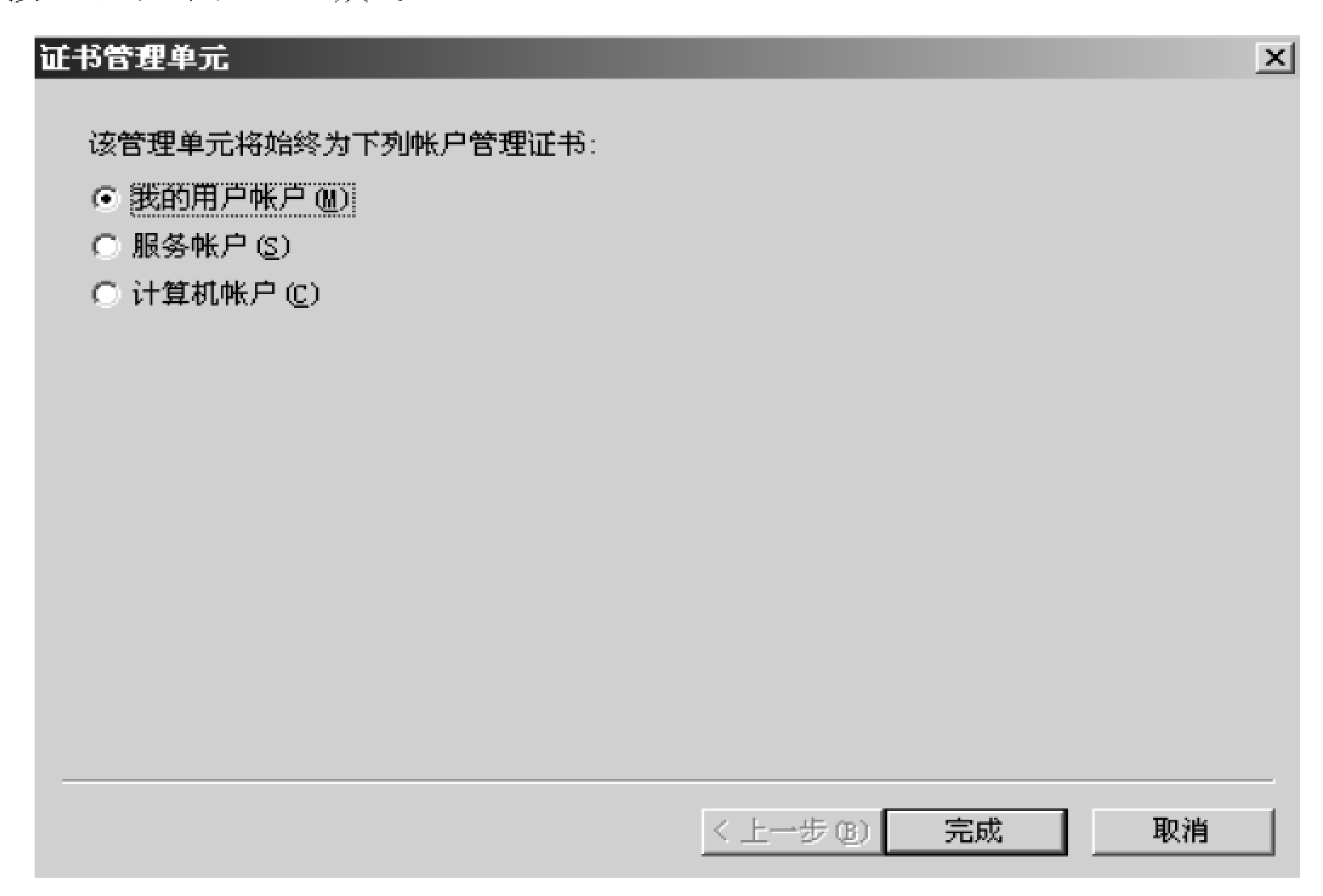


图 6-21　账户管理

❼ 选择【证书-当前用户】下的【个人】图标，右击，在弹出的快捷菜单中选择【所有任务】→【申请新证书】命令，弹出【证书申请向导】对话框，在欢迎页中单击【下一步】按钮，如图 6-22 所示。

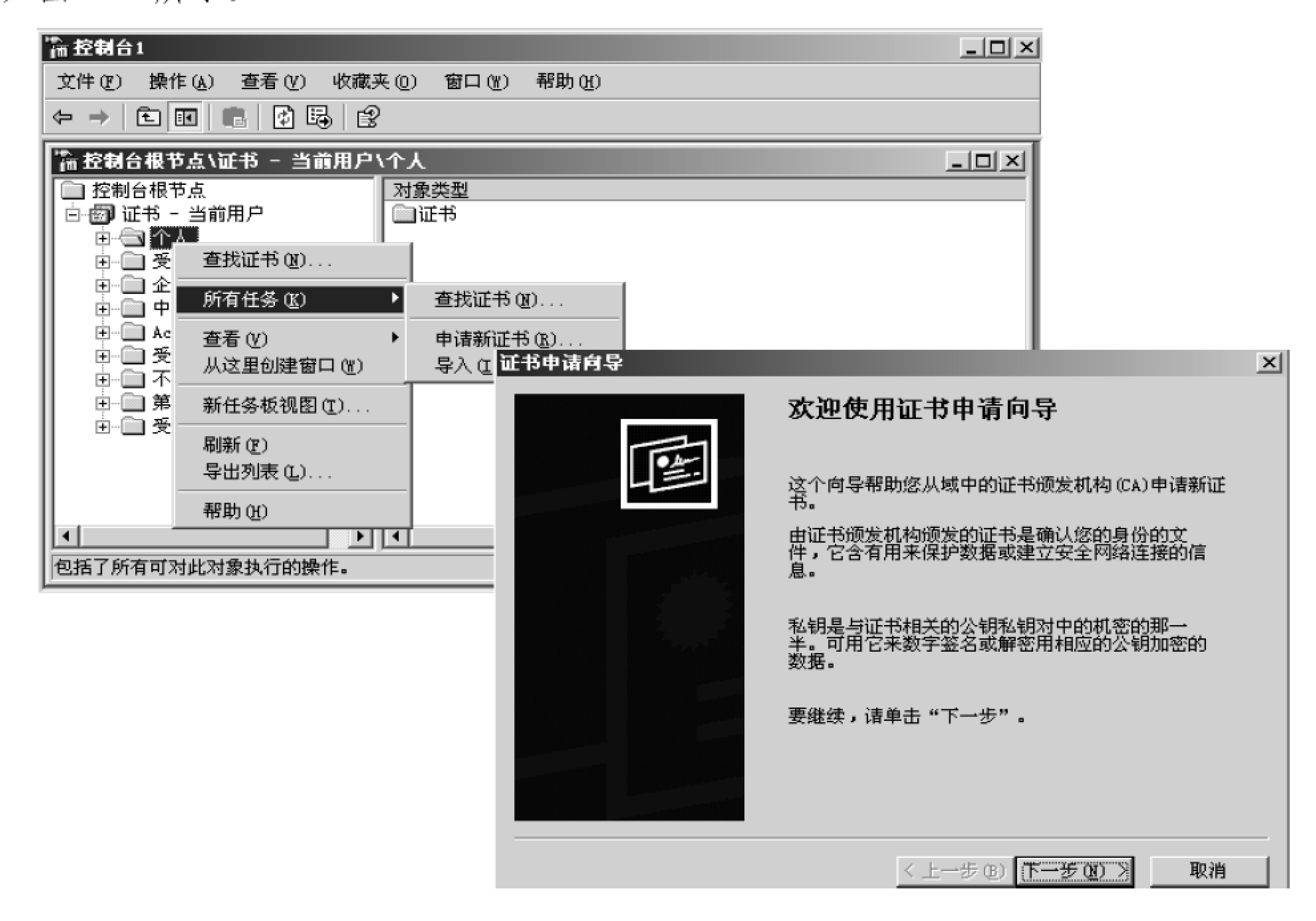


图 6-22　【证书申请向导】对话框

8 在【证书类型】向导页中，选择申请证书的类型。如果选中【高级】复选框，将会弹出【加密服务提供程序】向导页，让用户选择加密形式。Windows 自带了两种加密程序：一种是 Microsoft Base Cryptographic Provider；另一种是 Microsoft Enhanced Cryptographic Provider。设置完毕后，单击【下一步】按钮，如图 6-23 所示。

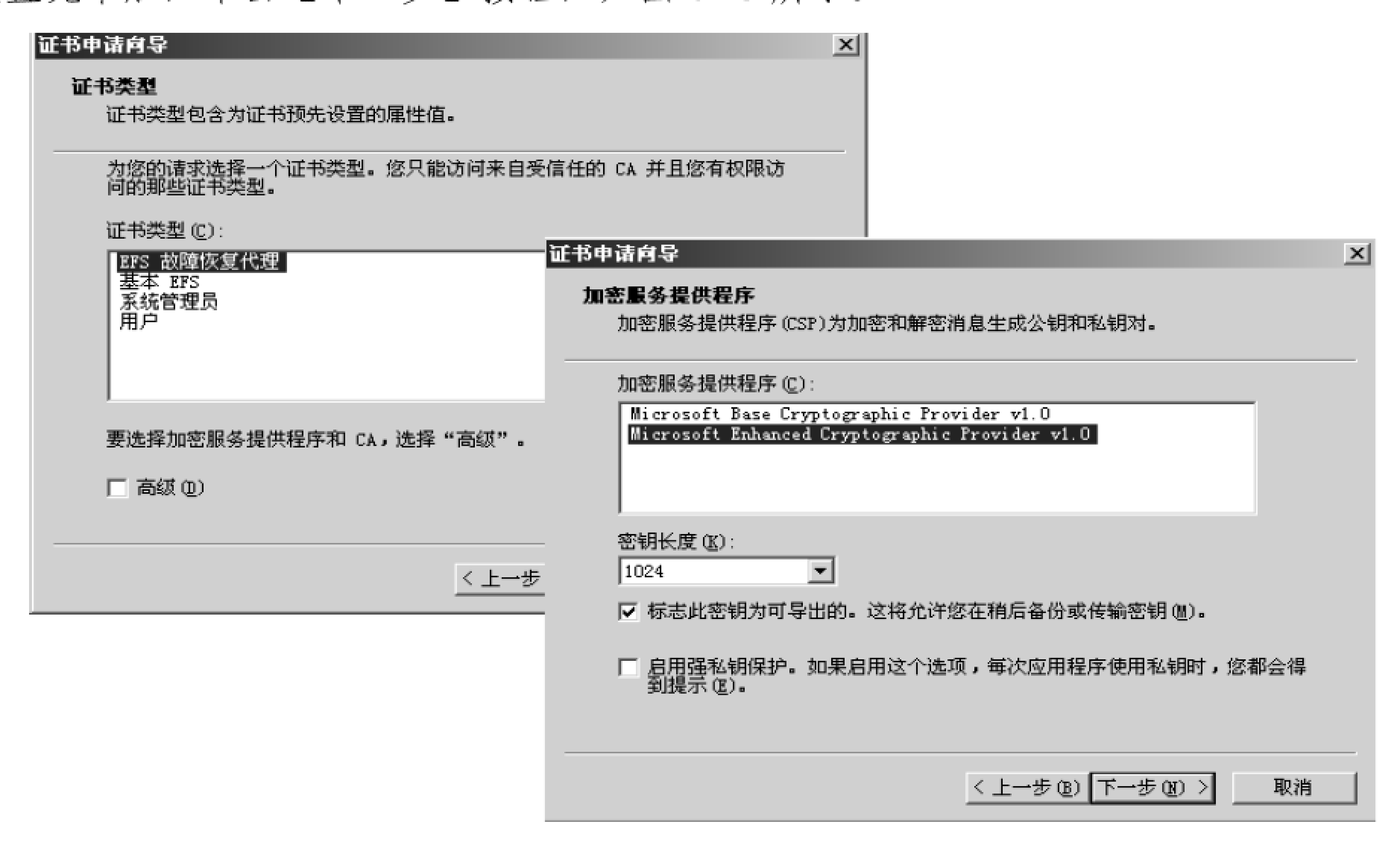


图 6-23　设置证书类型及加密类型

9 在【证书颁发机构】向导页中，保持默认设置，直接单击【下一步】按钮打开【证书的好记的名称和描述】向导页。如果有必要，证书应该在此加入一些简要的说明，用于识别。设置完毕后，单击【下一步】按钮，如图 6-24 所示。



图 6-24　设置证书颁发机构和好记的证书名称

❿ 在【正在完成证书申请向导】向导页中，单击【完成】按钮，如图 6-25 所示。



图 6-25　完成证书申请

3. Web 申请证书

Windows Server 2003 还提供了基于 Web 的证书申请和管理方式，默认情况下可以使用这些网页进行各种与证书服务相关的业务处理，其 URL 是：

```
http://证书服务器ip/certsrv
```

基于 Web 申请证书时，可以申请基本证书，也可以使用高级选项申请证书，并且可以选择不同的加密服务提供程序、不同的哈希算法(SHA/RSA，SHA/DSA，MD5)以及不同的密钥规格。用户可以将申请到的证书保存到 PKCS#10 文件中，其过程如下。

❶ 打开 Internet Explorer 浏览器，在地址栏输入证书服务器的 URL，服务器会询问身份，输入合法的用户名和密码，如图 6-26 所示。

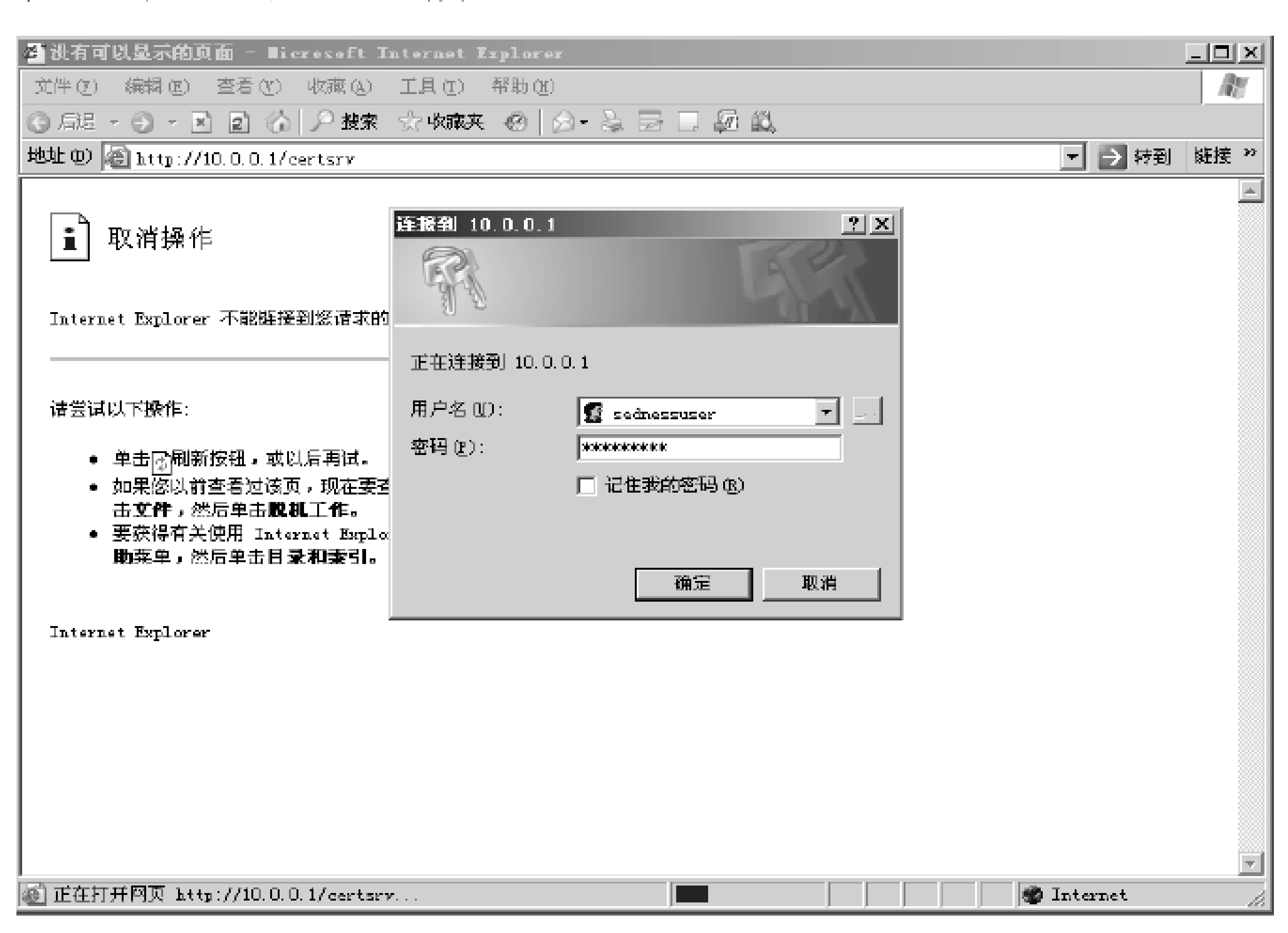


图 6-26　输入合法的用户名和密码

❷ 用户身份验证通过后，将打开证书服务站点的首页。单击【申请一个证书】链接，开始申

请证书，如图 6-27 所示。

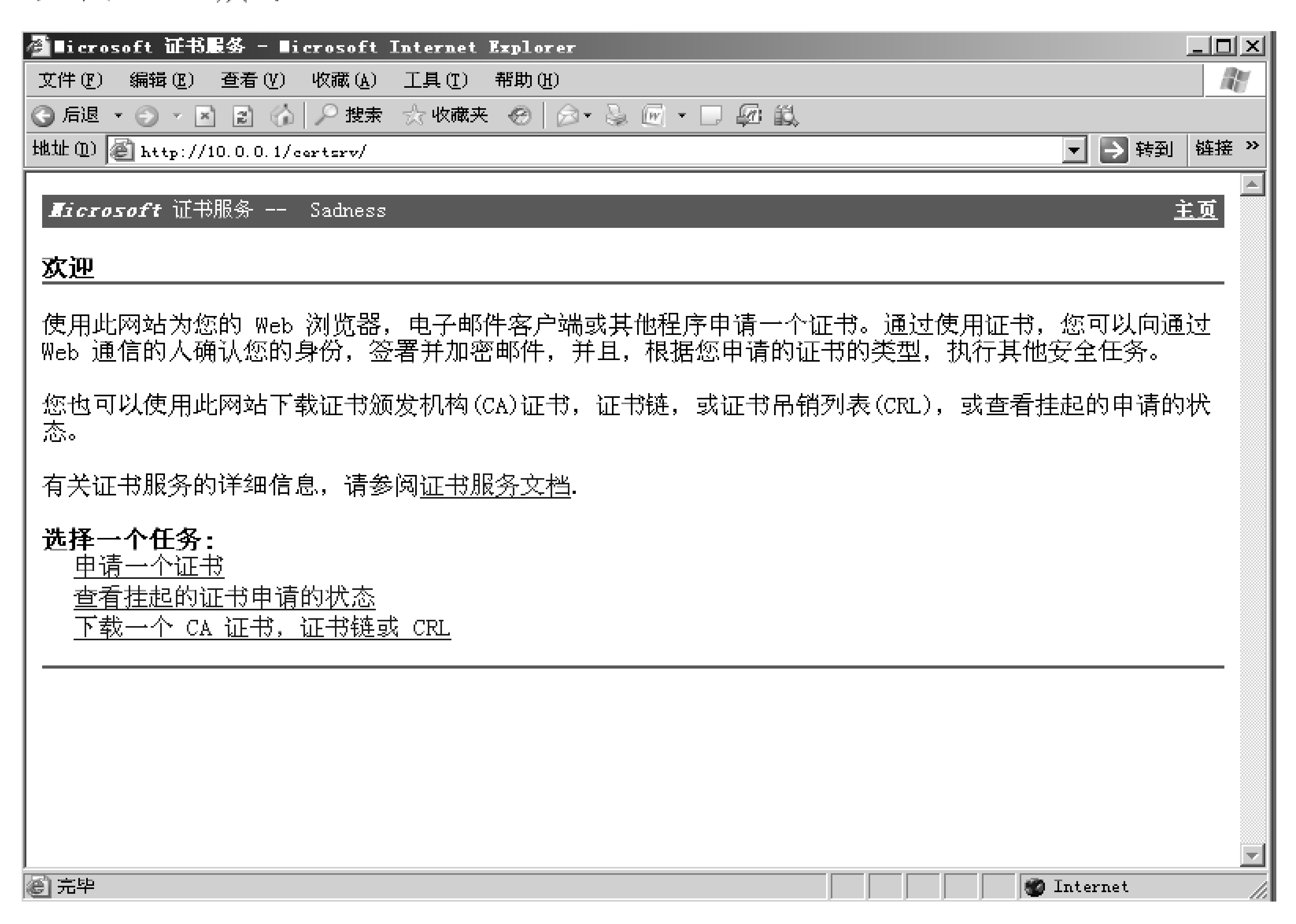


图 6-27　在打开的证书服务站点申请一个证书

❸ 在【申请一个证书】网页中，单击【用户证书】链接，如图 6-28 所示。



图 6-28　用户证书申请

❹ 在【用户证书–识别信息】网页中，单击【提交】按钮继续，或者单击【更多选项】链接来选择加密服务提供程序，设置是否启用强私钥保护以及申请格式，如图 6-29 所示。



图 6-29　设置用户证书-识别信息

❺ 单击【提交】按钮后，将会生成证书，并且会弹出【潜在的脚本冲突】安全信息提示框，告知“存在潜在的脚本冲突”，单击【是】按钮，如图 6-30 所示。



图 6-30　脚本冲突警告消息

❻ 证书生成后，系统会显示用户已经完成了证书的申请。如果原来已经安装了证书则会显示【证书已颁发】界面，如图 6-31 所示。



图 6-31 完成证书申请

❼ 在证书申请过程中，也可以在图 6-29 中单击【请使用“高级证书申请”窗体】链接，打开如图 6-32 所示的【高级证书申请】页面。

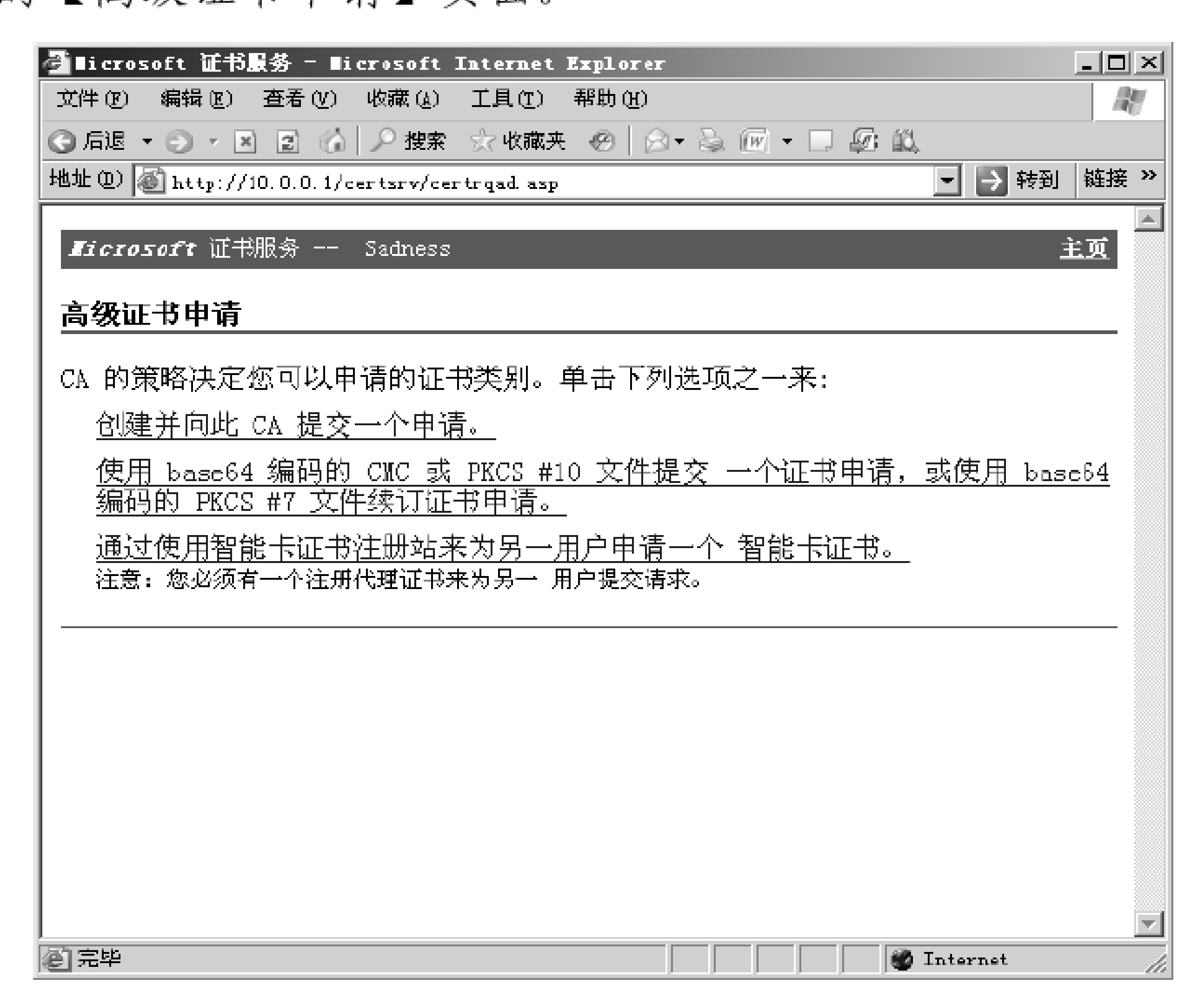


图 6-32 高级证书申请

❽ 单击【创建并向此 CA 提交一个申请】链接，进入【高级证书申请】网页，用户可以定义证书的各种高级属性，如图 6-33 所示。对于此页的各个选项的解释如下。

✧ CSP(Microsoft Enhanced Cryptographie Service Provider，加密服务提供程序)：设置 CSP 进行创建密钥、吊销密钥以及使用密钥执行各种加密操作。每个 CSP 都提供了不同的 CryptoAPI 实现。某些提供了更强大的加密算法，而另一些则使用硬件组件，例如智能卡。



图 6-33　高级证书申请

✧ 密钥大小：设置证书上公钥的长度(以位为单位)。通常，密钥越长越安全。

✧ 哈希算法：好的哈希算法使得构造两个相互独立且具有相同哈希的输入不能通过计算方法实现。典型的哈希算法包括 MD2、MD4、MD5 和 SHA-1。

✧ 密钥用法：设置如何使用私钥。【交换】表示私钥可以用于交换敏感信息。【签名】表示私钥只能用来创建数字签名。【二者】表示私钥可以用于交换和签名功能。

✧ 创建新密钥集/使用现存的密钥集：您用户可以将存储在计算机中的现有公钥和私钥对用于证书，或者为证书创建新的公钥和私钥对。有关重用密钥和生成新密钥的详细信息，请参阅证书资源上的内容。

✧ 启用强私钥保护：如果启用强私钥保护，每次需要使用私钥时，系统将提示用户输入密码。

✧ 标记密钥为可导出：如果将密钥标记为可导出，就能把公钥和私钥保存到文件中。在更改计算机并需要移动密钥对时，或删除密钥对并将它们保存在其他位置时，这是很有用的。

- ✧ 将证书保存在本地计算机存储中：如果当其他用户登录时，计算机需要访问与证书关联的私钥，则要选择该选项。当申请颁发给计算机(例如 Web 服务器)的证书，而不是颁发给用户的证书时，请选择该选项。
- ✧ 保存申请到一个文件：如果无法连接能够联机处理证书申请的证书颁发机构，则需要使用该选项。

❾ 完成以上选项的配置后，单击【提交】按钮完成申请。

4. 自动注册

上述手动申请和安装证书的过程我们可以将其看成为一种注册行为。但是对于大型网络而言，这样做十分复杂。证书自动注册是一个允许客户端自动向 CA 提交证书申请并允许检索和存储颁发证书的过程，整个过程由网络管理员进行控制。

使用自动注册功能，单位能够对用户证书的生命周期进行管理，包括证书续订、证书的取代和多个签名要求。

证书自动注册基于组策略设置和版本 2 证书模板的组合。这种组合使 Windows XP Professional 或 Windows Server 2003 客户端可以在用户登录到域时注册用户，或在计算机启动时注册该计算机，并使用户和计算机在这些事件之间定期更新。

自动注册用户证书提供了一种快捷简单的方式，用以向用户颁发证书和在 Active Directory 目录服务环境中启用公钥基础结构 (PKI) 应用程序，诸如智能卡登录、加密文件系统 (EFS)、安全套接字层 (SSL)、安全/多用途 Internet 邮件扩展(S/MIME)等。当 Windows XP Professional 客户端被配置为使用 Active Directory 时，用户自动注册可将标准 PKI 部署的高昂成本降到最低，并减少 PKI 实现的总拥有成本 (TCO)。下面简要地介绍一下证书自动注册的配置过程。

❶ 在【Active Directory 站点和服务】目录树中选择一个证书模板，右击，在弹出的快捷菜单中选择【属性】命令，打开证书模板的属性对话框，如图 6-34 所示。

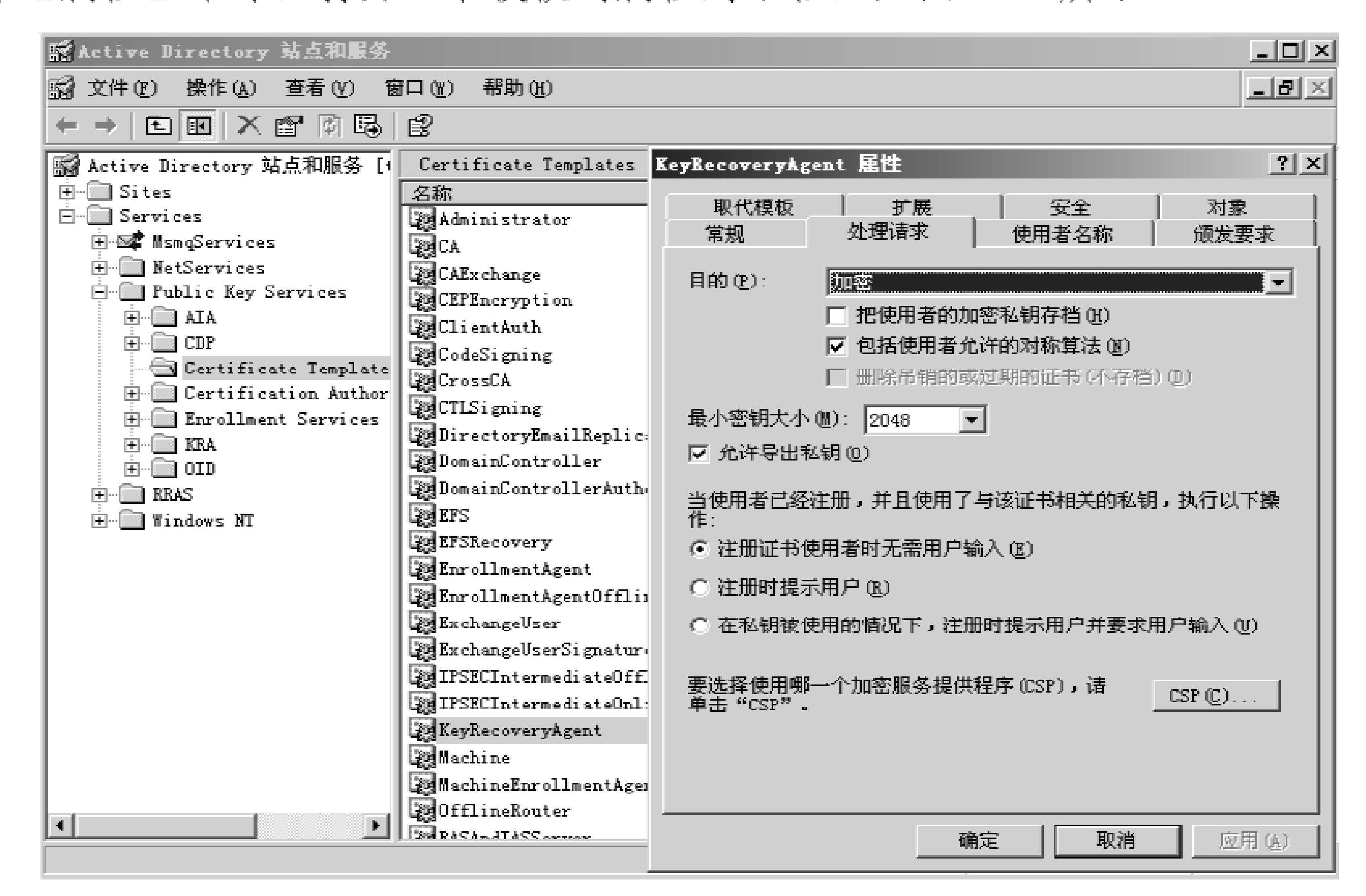


图 6-34 证书模板属性对话框

❷ 当然，并不是所有的证书都有相同的【处理请求】选项卡，如图 6-35 所示。



图 6-35　不同模板的【处理请求】选项卡

❸ 在所选证书模板的【处理请求】选项卡中单击 CSP 按钮，从弹出的【CSP 选择】对话框中选择 CSP 以改变智能卡模板的自动注册行为。如果选择了多个 CSP，那么，当 Windows XP 检索自动注册的证书并开始将它安装在智能卡上时，用户可能打开多个对话框。建议从该列表框中只为每个模板选择一个 CSP(加密服务提供程序)，如图 6-36 所示。

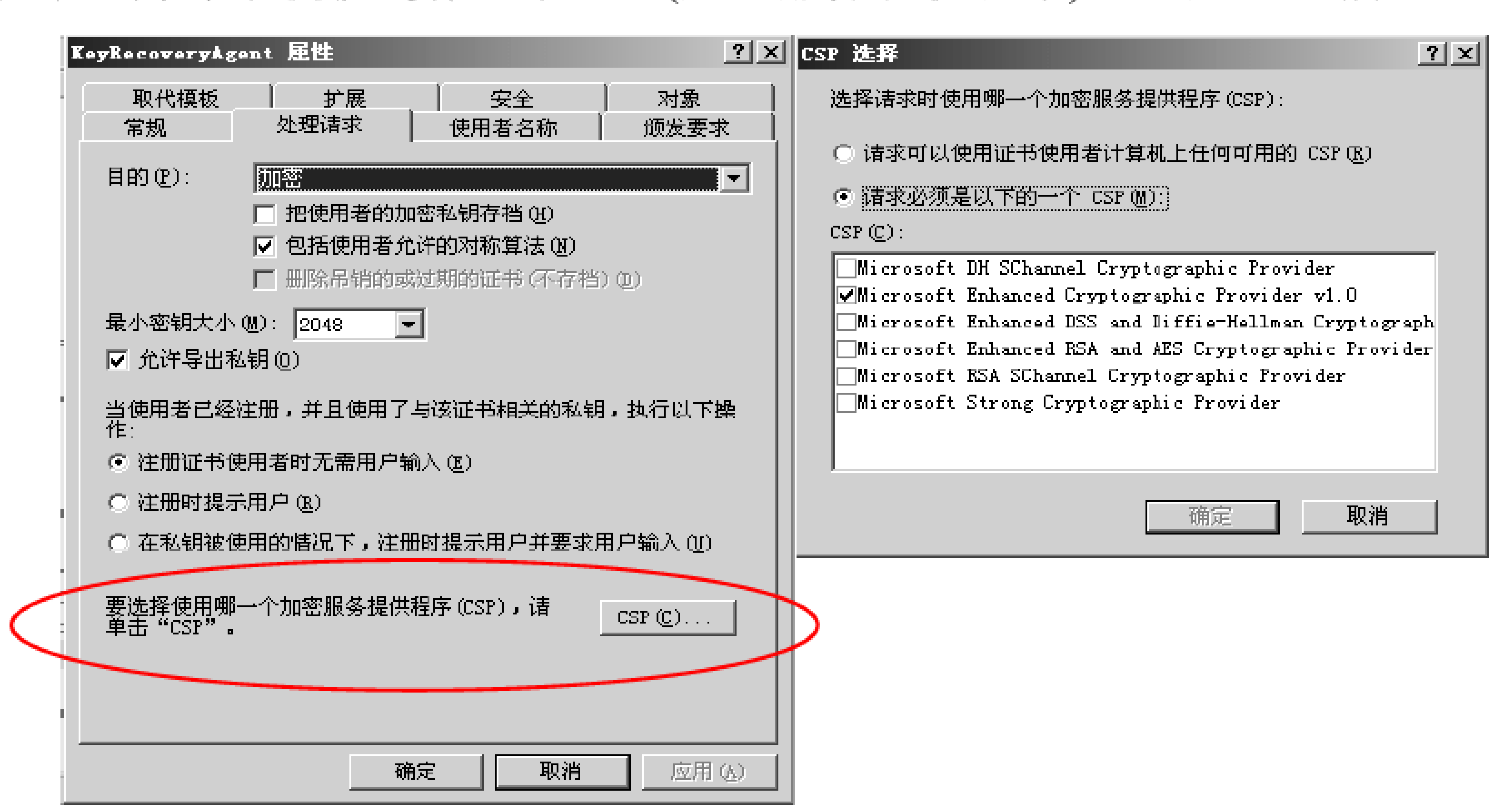


图 6-36　选择 CSP

❹ 在所选证书模板的【颁发要求】选项卡上，如果选中【授权签名的数量】复选框并使该值大于 1，将使接收方不能基于该模板自动注册，将需要请求者使用来自其证书存储中的有效证书的私钥来签署请求。该证书必须包含相同选项卡上的【应用程序策略】下拉列表框和

【颁发策略】列表框中所指定的应用程序策略和颁发策略。如果请求者的证书存储中存在合适的证书，则自动注册将使用该证书的私钥来签署该请求，并自动获得安装所请求的证书。在所选证书模板的【颁发要求】选项卡上，选中【有效的现存证书】单选按钮可能影响接收方自动注册。该单选按钮将告诉 CA 接收方在续订有效证书时不需要满足颁发要求。但已经无法自动注册初始证书的接收方才有可能能够使用自动注册来续订证书，如　图 6-37 所示。



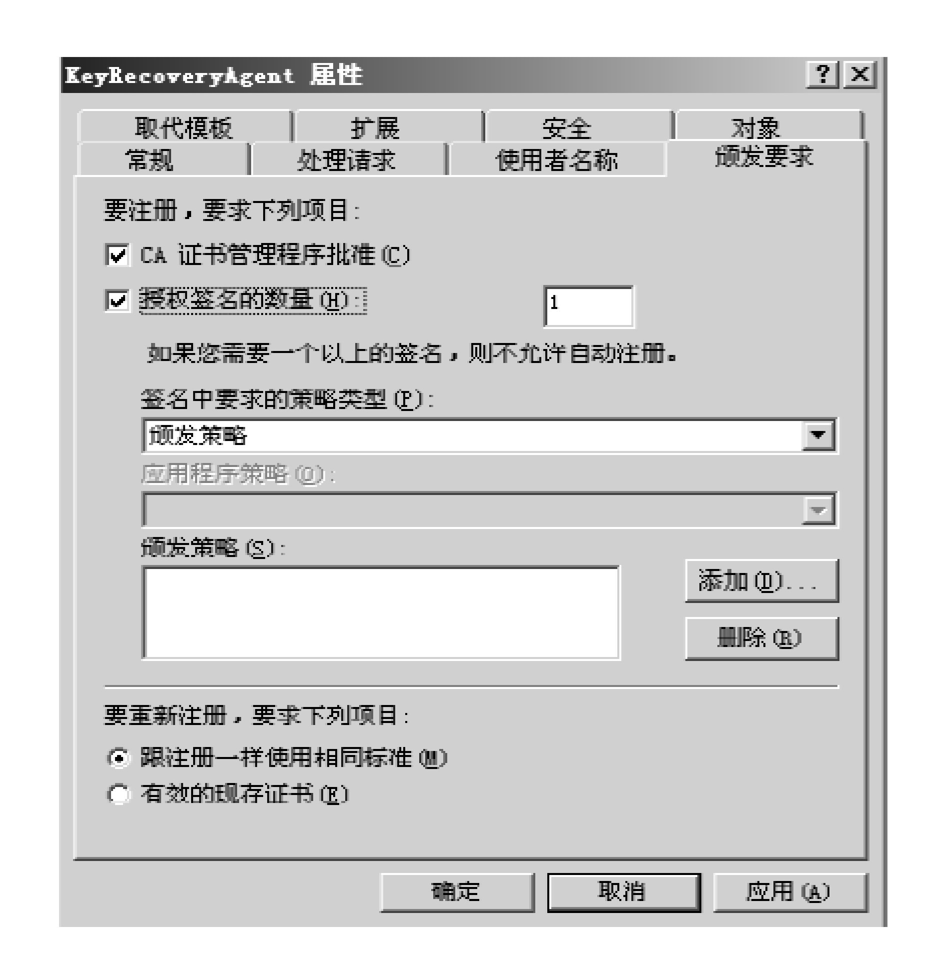


图 6-37　配置【使用者名称】和【颁发要求】选项卡

❺ 在所选证书模板的【常规】选项卡上，【有效期】和【续订期】指定了证书的有效证书期限，以及在它的有效期限结束之前多长时间自动注册将请求续订，如图 6-38 所示。由于有效期可以非常短，并且续订期可能重叠，因此，自动注册将在已经过了证书有效期至少 20%之后才会续订证书。这样可以防止由于有效期和续订期设置被错误配置，而导致自动注册无休止地续订证书。



图 6-38　配置有效期和续订期

❻ 依次单击【开始】→【运行】菜单，在打开的【运行】对话框中输入 mmc 命令，单击【确定】按钮进入【控制台】窗口，然后选择【文件】→【添加/删除管理单元】命令，如图 6-39 所示。



图 6-39 【控制台】窗口

❼ 在【添加/删除管理单元】对话框中，单击【添加】按钮；并在【添加独立管理单元】对话框中，选择【证书模板】选项，再单击【添加】按钮，如图 6-40 所示。

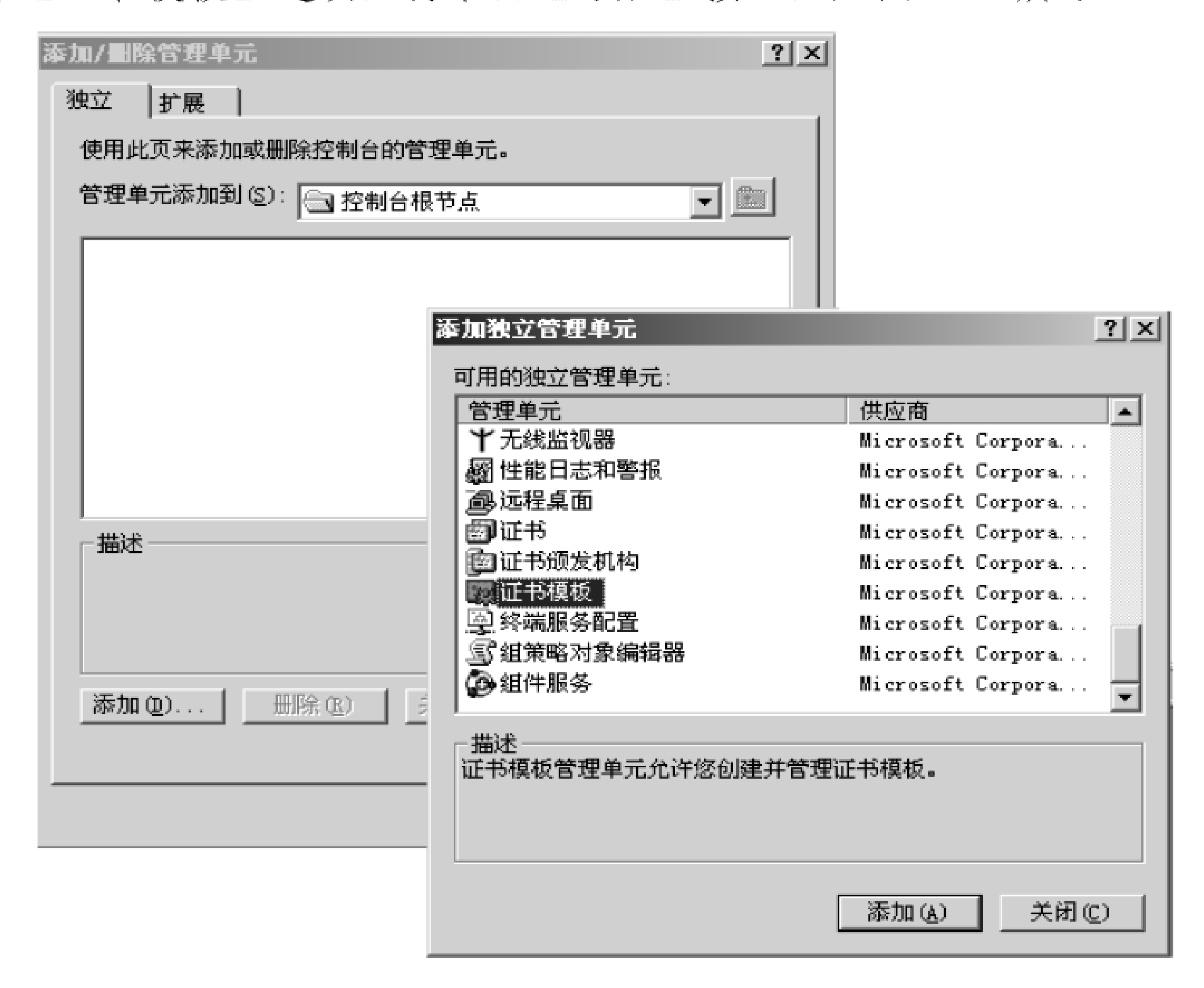


图 6-40 【添加独立管理单元】对话框

❽ 添加完成后，单击控制台左侧窗格中【证书模板】选项，并在其右窗格选择【用户】模板，然后选择【操作】→【复制模板】命令，如图 6-41 所示。

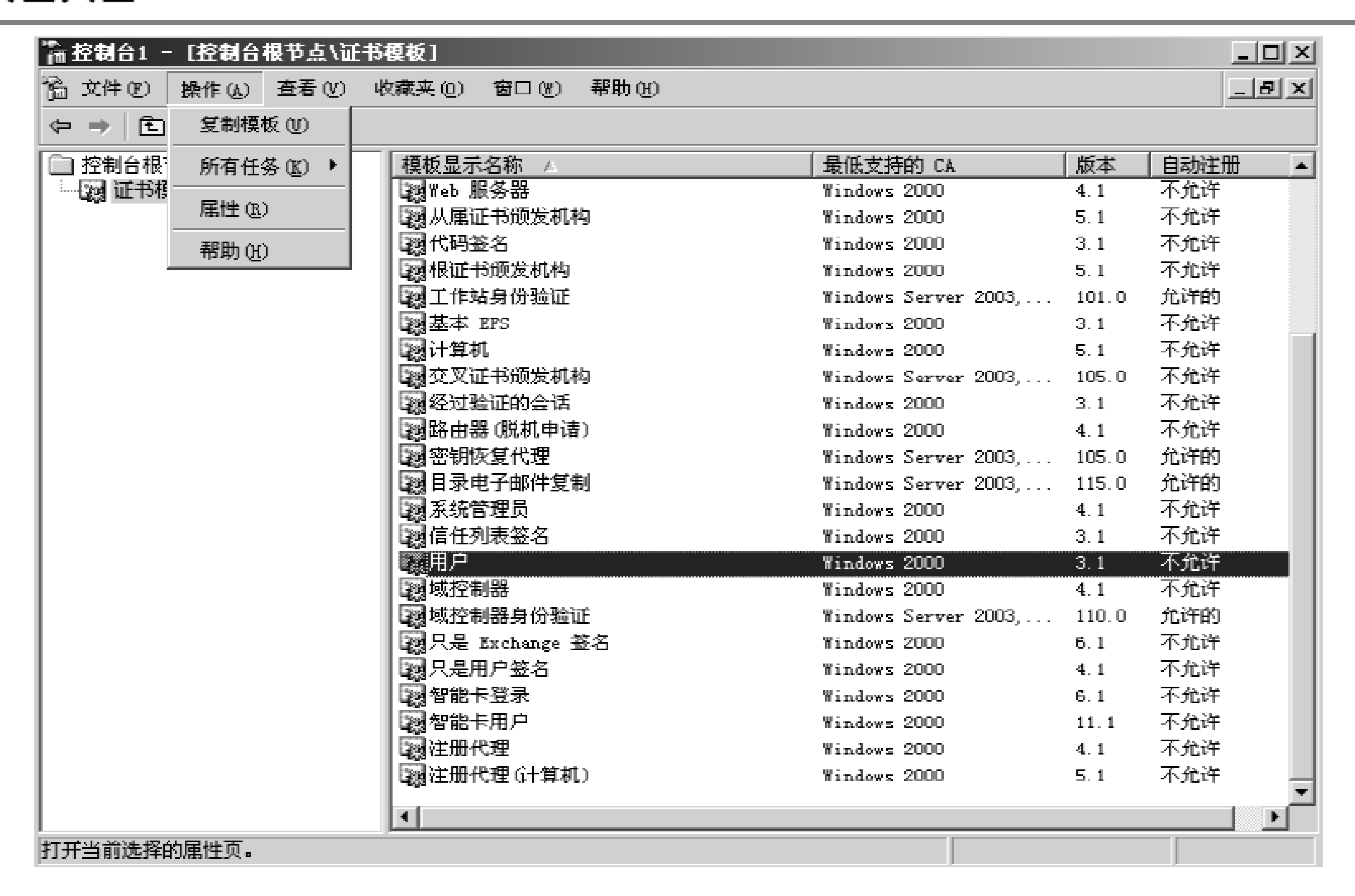


图 6-41　复制证书模板

❾ 在【新模板的属性】对话框的【常规】选项卡中，选中【在 Active Directory 中颁发证书】复选框，然后切换到【安全】选项卡，在【组或用户名称】列表框中选择 Domain Users 选项，在 Domain Users 的权限框中选择【注册】和【自动注册】两个复选框，如图 6-42 所示。

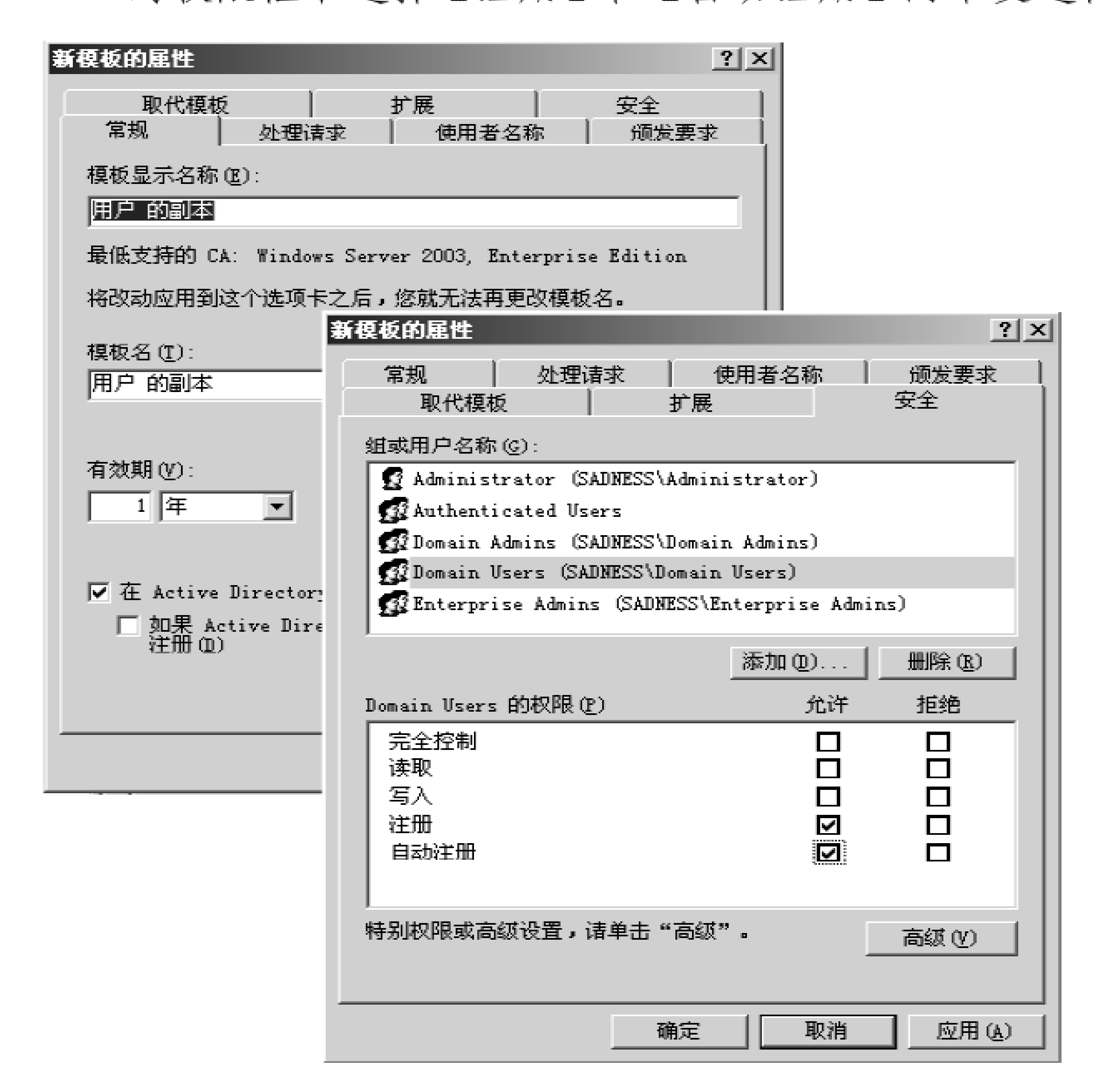


图 6-42　设置模板权限

❿ 依次单击【开始】→【程序】→【管理工具】→【证书颁发机构】菜单，在控制台中选择【证书模板】选项，然后选择【操作】→【新建】→【要颁发的证书模板】命令，如图 6-43 所示。



图 6-43　新建要颁发的证书模板

⓫ 在【启用证书模板】对话框中，选择刚才新建的用户证书模板的副本，然后单击【确定】按钮，如图 6-44 所示。

⓬ 依次单击【开始】→【运行】命令，在【运行】对话框中输入 mmc，进入【控制台】窗口，然后单击【文件】→【添加删除管理单元】命令，在打开的【添加独立管理单元】对话框中选择【Active Directory 用户和计算机】选项，如图 6-45 所示。

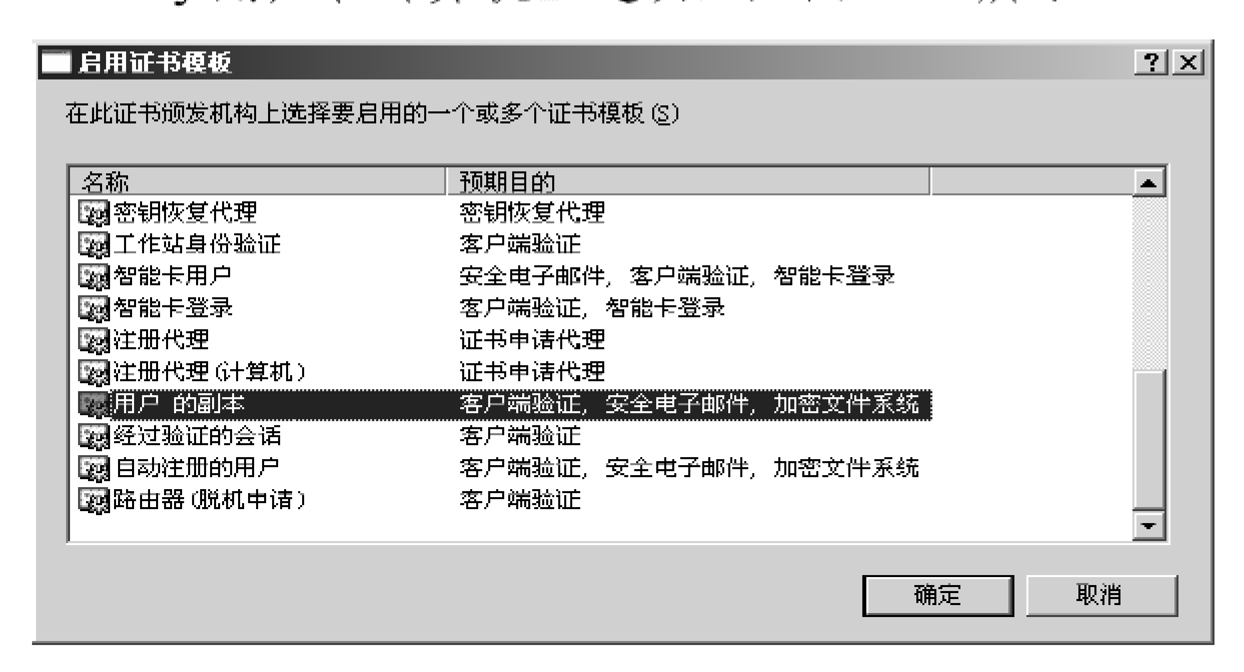


图 6-44　选择用户证书模板



图 6-45　添加 Active Directory 用户和计算机

⓭ 在控制台中对所选的域(例如下图中的 sadness 域)单击右键，在弹出的快捷菜单中，选择【属性】命令，并切换到【组策略】选项卡，如图 6-46 所示。



图 6-46 【组策略】选项卡

⓮ 单击【编辑】按钮，在新弹出的【组策略编辑器】窗口中选择【用户配置】→【Windows 设置】→【安全设置】→【公钥策略】，单击【自动注册设置】，并在弹出的【自动注册设置 属性】对话框中选中【续订过期证书、更新未决证书并删除吊销的证书】和【更新使用证书模板的证书】复选框，如图 6-47 所示。

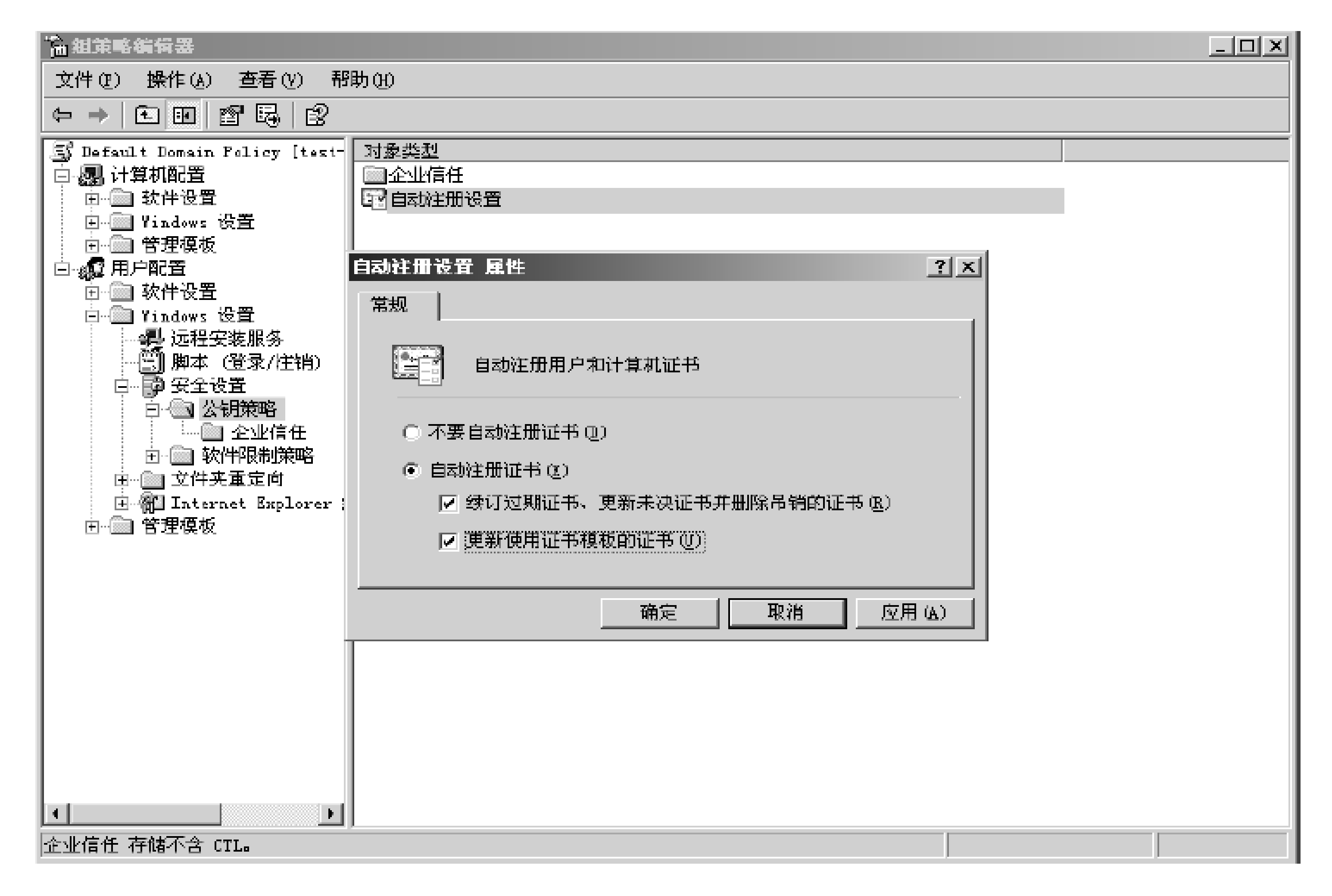


图 6-47 自动注册设置

通过上述步骤，我们完成了一个 CA 的安装和配置工作，并且也实现了手工证书申请、基于 Web 证书申请和自动证书申请的配置。下面两节，我们将介绍如何吊销证书以及如何导入和导出证书。

6.1.4　证书吊销

应用实例导航：Sadness 公司证书系统管理

※场景呈现

Sadness 公司根据我们的建议建立了一套安全完善的证书管理系统，但是前一章所述的那个攻击者利用公司证书管理员的疏忽，继续使用证书服务访问公司内部的大量资源。因此 Sadness 公司为了维护单位的 PKI 完整性，在受领证书的员工离开单位后，或者某个证书泄密后，应当由 CA 的管理员将其证书吊销，当证书被 CA 吊销时，它将添加到该 CA 的证书吊销列表(CRL)中，可采取新的 CRL 或增量 CRL 的形式进行该操作。增量 CRL 是一个小的 CRL，列出自上一个完整的 CRL 以来吊销的证书。

※技术要领

(1) 吊销证书；
(2) 安排证书吊销列表(CRL) 的发布；
(3) 吊销大量证书。

对于证书吊销，通常有如下几个原因。

✧ 证书受领人的私钥泄露或被怀疑泄露；
✧ 证书颁发机构的私钥泄露或被怀疑泄露；
✧ 发现证书是用欺骗手段获得的；
✧ 作为信任实体的证书受领人的状态改变；
✧ 更改证书受领人的名称。

公钥基础结构(PKI)取决于凭据的分布式验证，这样就不必与保护凭证安全的中央信任实体直接通信。这样就需要将证书吊销信息分发给个人、计算机和正在尝试验证证书有效性的应用程序。对吊销信息及其时间性的要求取决于证书吊销检查的应用程序及其执行情况。要有效支持证书吊销，客户端必须确定证书是否有效或是否被吊销。为支持各种方案，证书服务支持证书吊销的行业标准方法，包括在客户端能够访问的多个位置(包括 Active Directory 目录服务、Web 服务器和网络文件共享)上发布证书吊销列表(CRL)和增量 CRL。

CRL 是已经吊销的未过期证书的完整的数字签名列表。客户端检索该列表，将其缓存(根据配置的 CRL 的寿命)并使用它来验证所提供的要使用的证书。由于 CRL 会变大，根据证书颁发机构的大小，也可发布增量 CRL。增量 CRL 只包含自发布上一个基本 CRL 以来吊销的证书。它允许客户端检索较小的增量 CRL 并快速建立完整的已吊销证书列表。使用增量 CRL 也允许进行更加频繁的发布，因为增量 CRL 的大小需要的开销小于完整的 CRL 的开销。

1. 吊销证书

下面简要地介绍一下吊销证书的操作步骤。

❶ 在证书服务器中，依次选择【开始】→【程序】→【管理工具】→【证书颁发机构】，打开【证书颁发机构】管理控制台窗口。在证书颁发机构控制树中选择【颁发的证书】选项，如图 6-48 所示。

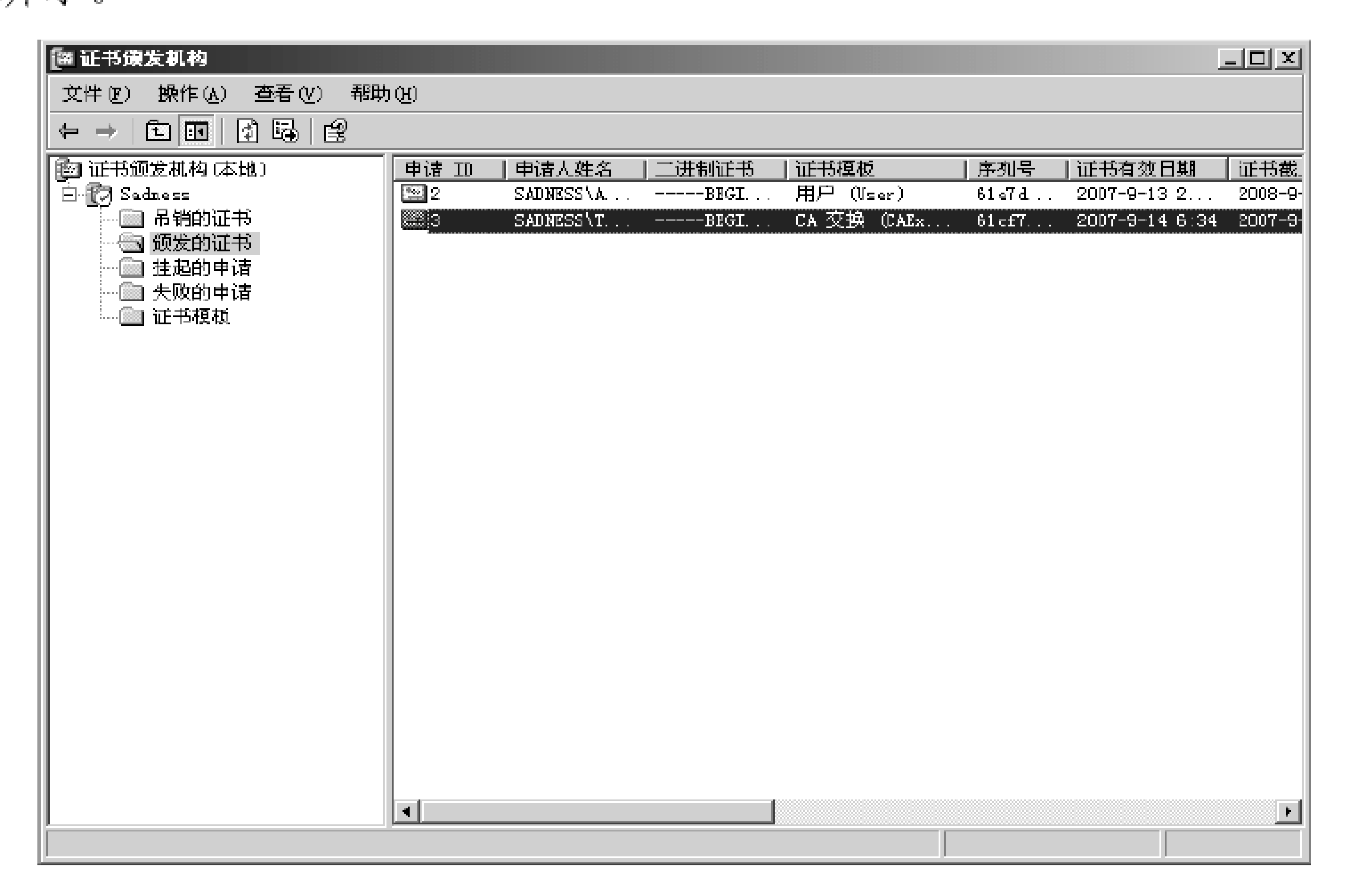


图 6-48 查看证书

❷ 在右窗格中选择需要吊销的证书，并右击，在弹出的快捷菜单中选择【所有任务】→【吊销证书】命令。在弹出的【证书吊销】对话框中，选择吊销证书的理由。若在【理由码】下拉列表框中选择【证书待定】，则在证书到期前都可以取消证书吊销。如果证书状态不能肯定，而且要给 CA 管理员提供一些灵活性，则选择该选项非常有用，如图 6-49 所示。



图 6-49 吊销证书

❸ 如果从“证书待定”状态撤销已吊销的证书，可在 CA 命令提示符下执行如下命令。

```
certutil -revoke CertificateSerialNumber unrevoke
```

❹ 如果想对原因代码为“证书待定”状态的吊销证书更改吊销类型，请在 CA 命令提示符下输入如下命令，其中 Code 定义如表 6-2 所示。

```
certutil -revoke CertificateSerialNumber Code
```

表 6-2　Code 定义

新原因代码	命　令
未指定	certutil -revokeCertificateSerialNumber 0
密钥泄漏	certutil -revokeCertificateSerialNumber 1
CA 泄漏	certutil -revokeCertificateSerialNumber 2
附属关系已改变	certutil -revokeCertificateSerialNumber 3
被取代	certutil -revokeCertificateSerialNumber 4
操作停止	certutil –revokeCertificateSerialNumber 5

2. 安排证书吊销列表(CRL)的发布

证书服务的其中一项功能是，在 CA 管理员指定了时间间隔后，每个 CA 都自动发布更新的 CRL，该时间间隔称为“CRL 发布期”。在初次安装 CA 之后，CRL 发布期被设置为一周(根据本地计算机时间，从 CA 首次安装的日期开始计算)。

CA 管理员应了解 CRL 发布期和 CRL 有效期之间的区别。CRL 的有效期是证书验证者将 CRL 视为权威的时间段。只要证书验证者在其本地缓存中具有有效的 CRL，它就不会尝试从发布它的 CA 检索另一个 CRL。

CRL 的发布期由 CA 管理员建立。但是，CRL 的有效期是从发布期延伸而来的，期间允许进行 Active Directory 复制。在默认情况下，证书服务将发布期延长 10%(最多可加上 12 个小时)以建立有效期。因此，如果 CA 每 24 小时发布 CRL，那么有效期设置为 26.4 小时。

此外，还存在时钟偏差(在发布期的开始和结束时间额外增加 10 分钟)。因此考虑到计算机时钟设置中的偏差，CRL 将在其发布期开始前 10 分钟有效。管理员还可使用注册表项来控制发布期和有效期之间的差异，以便更慢的目录复制也能顺利进行。

确定 CRL 发布的计划时，应对性能与安全性进行平衡。发布 CRL 的频率越高，当前客户端使用已吊销 CRL 列表的次数越多，它们接收最近吊销的证书的可能性越小。但是，频繁发布会对网络和客户端的性能造成不良影响。要减轻这种不平衡性，可在环境支持的情况下使用增量 CRL。

下面简要地介绍安排证书吊销列表(CRL)的发布的配置过程。

❶ 在【证书颁发机构】管理控制台窗口的控制树中，选择【吊销的证书】选项，右击，在弹出的快捷菜单中选择【属性】命令，如图 6-50 所示。

❷ 在【吊销的证书 属性】对话框中，设置【CRL 发布间隔】以及是否发布增量 CRL，然后单击【确定】按钮完成配置，如图 6-51 所示。

3. 吊销大量证书

在进行大量证书吊销的大型 CA 上，CRL 可以变得很长。对于频繁下载的客户端来说，

这会成为一种负担。要将很长的 CRL 的频繁下载次数降至最低，可发布增量 CRL。它使客户端能够下载最新增量 CRL，并将该 CRL 与最新基本 CRL 组合在一起，以拥有已吊销证书的完整列表。由于客户端通常在本地缓存 CRL，因此，使用增量 CRL 可潜在改进性能。

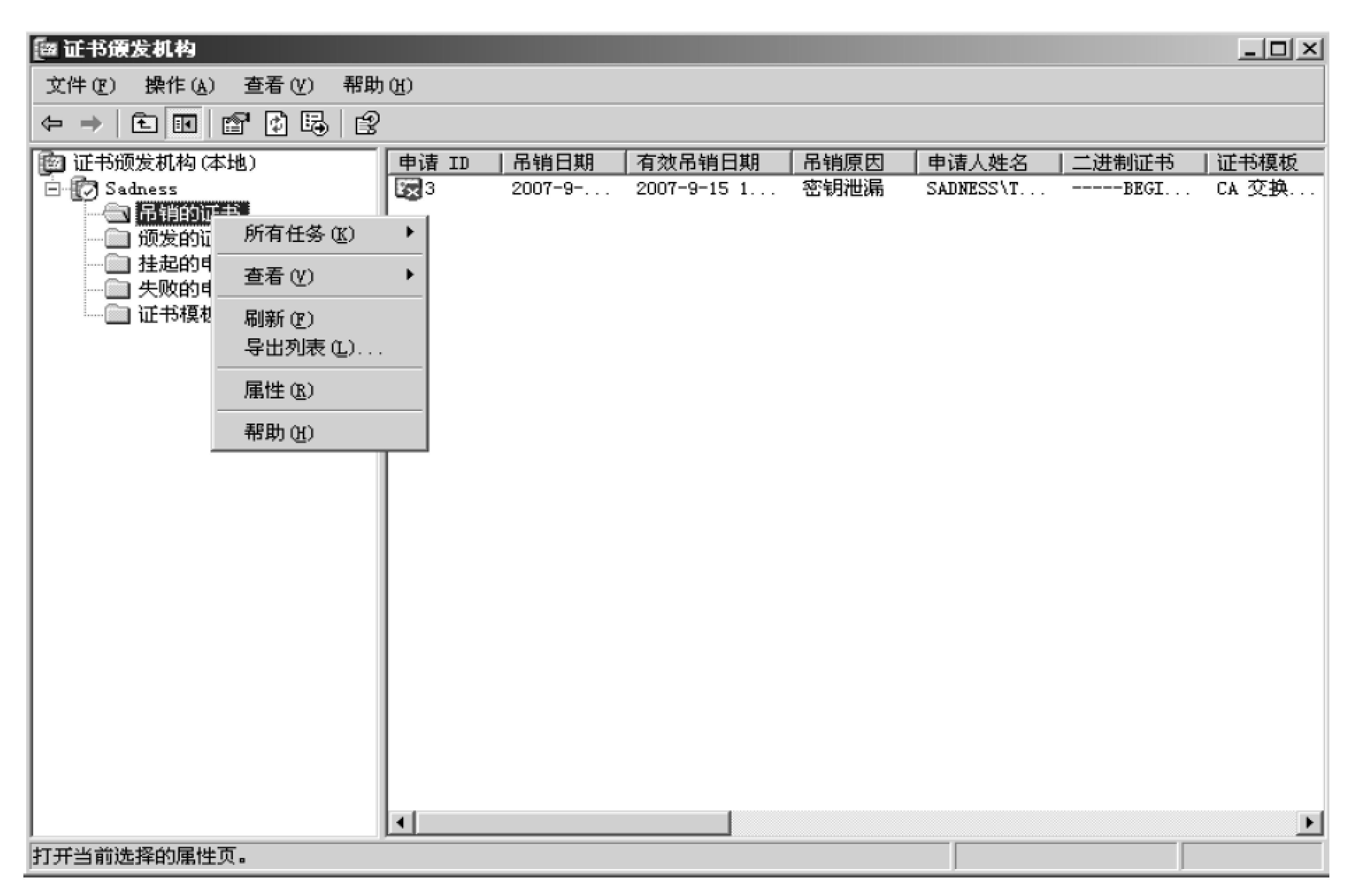


图 6-50　设置吊销证书属性

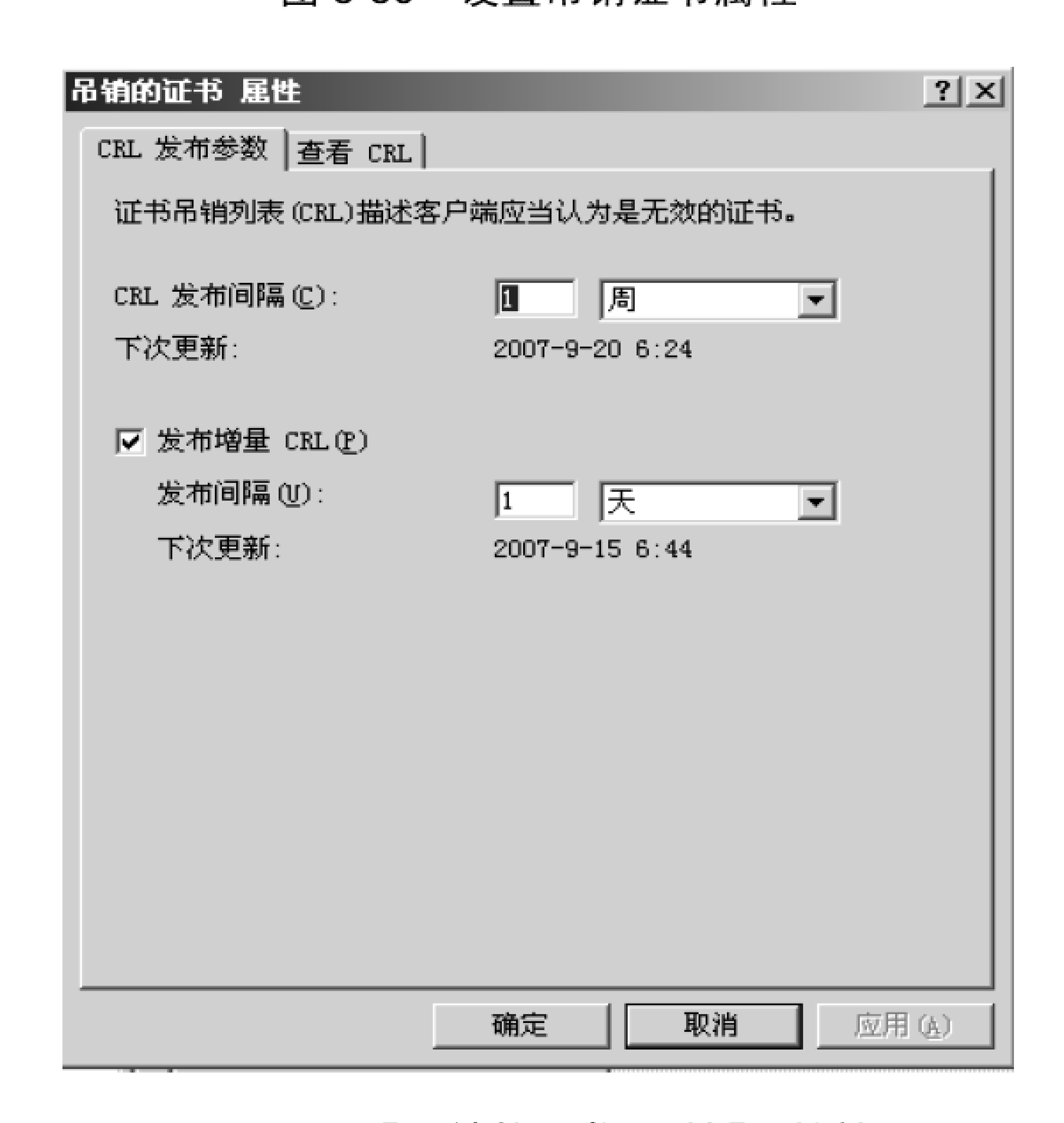


图 6-51　【吊销的证书 属性】对话框

要使用增量 CRL，客户端应用程序必须了解并明确使用增量 CRL 来进行吊销检查。如果客户端不使用增量 CRL，它会在每次刷新其缓存时从 CA 检索 CRL，不管增量 CRL 是否存在。为此，应验证预期应用程序是否使用增量 CRL，并进行相应的配置。如果客户端不支持使用增量 CRL，则不应将 CRL 配置为发布增量 CRL，或者不应将其配置为于同一间隔发布 CRL 和增量 CRL。这仍允许未来的支持增量 CRL 的应用程序使用它们，同时可为所有应用程序提供当前 CRL。注意，使用 Windows XP 和 Windows Server 2003 家族产品中的 CryptoAPI 的所有应用程序都使用增量 CRL。

要解决增量 CRL 非常大的这种特殊情况，可在 CA 上执行以下步骤。

❶ 在以下注册表项下修改注册表值。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configurati
on\<Name of CA>

// 将 CRLOverLapPeriod 设为分钟。默认值为小时。
// 将 ClockSkewMinutes 设为 1 分钟。默认值为 10。
```

❷ 重新启动 CA 服务。重新启动 CA 服务的方法是，打开【服务】控制台窗口，在窗口右侧列表框中，右击 Certificate Services，在弹出的快捷菜单中 选择【重新启动】命令，如图 6-52 所示。

❸ 发布新的基本 CRL。基本 CRL 具有仅两分钟的 CRLPropagationComplete 时间，所有后续增量 CRL 都参考此基本 CRL。一旦完成此项，便可以将 CRLOverLapPeriod 和 ClockSkew 恢复为默认值。



图 6-52　重新启动 CA

4. 手动发布 CRL

我们还可以根据需要随时发布 CRL，例如在重要证书的安全受到威胁时。选择在确定的计划外发布 CRL，将计划的发布期重设为在该时间开始。换句话说，如果在计划的发布期中间手动发布 CRL，会重新启动该 CRL 发布期。

❶ 在【证书颁发机构】管理控制台窗口的控制树中，选择【吊销的证书】选项，右击，在弹

出的快捷菜单中选择【所有任务】→【发布】命令，如图 6-53 所示。

图 6-53　手动发布 CRL

❷ 在【发布 CRL】对话框中，选中【新的 CRL】单选按钮，覆盖以前发布的证书吊销列表 (CRL)，或选中【仅增量 CRL】单选按钮来发布当前增量 CRL，并单击【确认】按钮。

点评与拓展：即使是已经发布了新的 CRL，具有以前发布的 CRL 缓存副本的客户端仍可以继续使用它直到有效期满，这一点非常重要。手动发布 CRL 不影响仍然有效 CRL 的缓存副本，它只为没有有效 CRL 缓存副本的系统提供新的 CRL。

6.1.5　证书导入、导出

证书管理提供了导出和导入证书的管理工具，如果需要，还可以包括证书路径和私钥。在不同的 CA 系统中，证书格式可以不同，如 PKCS #12 、PKCS #7 和 ITU-T X.509 等。

1. 标准证书格式

1)　个人信息交换

个人信息交换格式(PFX，也称为 PKCS #12)允许证书及相关私钥从一台计算机传输到另一台计算机或可移动媒体。

PKCS #12(公钥加密标准 #12)是业界格式，适用于证书及相关私钥的传输、备份和还原，该操作可以在相同或不同的供应商的产品之间进行。

要使用 PKCS #12 格式，加密服务提供程序 (CSP) 必须将证书和密钥识别为可以导出。如果证书是由 Windows Server 2003 或 Windows 2000 证书颁发机构颁发的，则在满足下列条件之一时，该证书的私钥将仅为可导出的。

✧　该证书用于加密文件系统 (EFS) 或 EFS 恢复。

✧ 通过在【高级证书申请】证书颁发机构的网页上选中【标记密钥为可导出】复选框，才能申请该证书。

因为导出私钥可能使私钥暴露给无关一方，所以 PKCS #12 格式是 Windows Server 2003 中支持的导出证书及相关私钥的唯一格式。

2) 加密消息语法标准

PKCS #7 格式允许将证书及证书路径中的所有证书从一台计算机传输到另一台计算机或可移动媒体。PKCS #7 文件通常使用 .p7b 扩展且与 ITU-T X.509 标准兼容。PKCS #7 允许一些属性(例如，反签名)与签名相关，而一些属性(例如，签名时间)可与消息内容一起验证。

3) DER 编码的二进制

ITU-T X.509 中定义的 ASN.1 DER(区别编码规则)与 ITU-T X.209 中定义的 ASN.1 BER(基本编码规则)相比，是一个限制更严格的编码标准，它构成了 DER 的基础。BER 和 DER 都提供了独立于平台的编码对象(如证书和消息)的方法，以便于其在设备和应用程序之间的传输。

在证书编码期间，多数应用程序都使用 DER，因为证书的一部分(CertificationRequest 的 CertificationRequestInfo)必须使用 DER 编码，才能对其进行签名。

不在运行 Windows Server 2003 计算机上的证书颁发机构也可能使用该格式，因此它支持互操作性。DER 证书文件使用 .cer 扩展名。

4) Base64 编码的 X.509

这种编码方式主要是为使用“安全 / 多用途 Internet 邮件扩展 (S/MIME)”而开发的(S/MIME 是一种通过 Internet 传输二进制附件的常用标准方法)。Base64 将文件编码为 ASCII 文本格式，这样可以减少传送的文件在通过 Internet 网关时被损坏的几率，同时，S/MIME 可以为电子消息发送应用程序提供一些加密安全服务，包括通过数字签名来证明原件(非拒绝)，通过加密、身份验证和消息完整性来保证隐私和数据安全。

MIME(多用途 Internet 邮件扩展)标准(RFC 1341 及其后继者)定义了为传送电子邮件而进行任意二进制信息编码的一种机制。

由于所有符合 MIME 标准的客户端都可以对 Base64 文件进行解码，不在运行 Windows Server 2003 计算机上的证书颁发机构也可以使用该格式，所以它支持互操作性。Base 64 证书文件使用 .cer 扩展名。

2. 导入数据证书

当下列情况发生时，我们需要导入数据证书。

✧ 安装包含在由另一个用户、计算机或证书颁发机构发送给用户文件中的证书。

✧ 还原受损或丢失的以前备份的证书。

✧ 从证书所有者以前使用过的计算机上安装证书及其关联的私钥。

下面简要地介绍一下导入数据证书的操作步骤。导入数据证书的操作步骤如下。

❶ 在【证书颁发机构】管理控制台窗口的控制树中，选择【个人】选项，右击，在弹出的快捷菜单中选择【所有任务】→【导入】命令，弹出【证书导入向导】对话框，如图 6-54 所示。



图 6-54　打开证书导入向导

❷ 进入【证书导入向导】对话框后，单击【下一步】按钮，如图 6-55 所示。



图 6-55　【证书导入向导】对话框

❸ 在【要导入的文件】向导页中，选择需要导入的证书文件，并单击【下一步】按钮，如图 6-56 所示。



图 6-56　选择需要导入的证书文件

❹ 在【证书存储】向导页中，选择证书存放位置。如果要根据证书类型将证书自动放置在证书存储区中，选中【根据证书类型，自动选择证书存储】单选按钮；如果要指定存储证书的位置，选中【将所有的证书放入下列存储】单选按钮。单击【浏览】按钮，然后选择要使用的证书存储区。设置完毕后，单击【下一步】按钮，如图 6-57 所示。

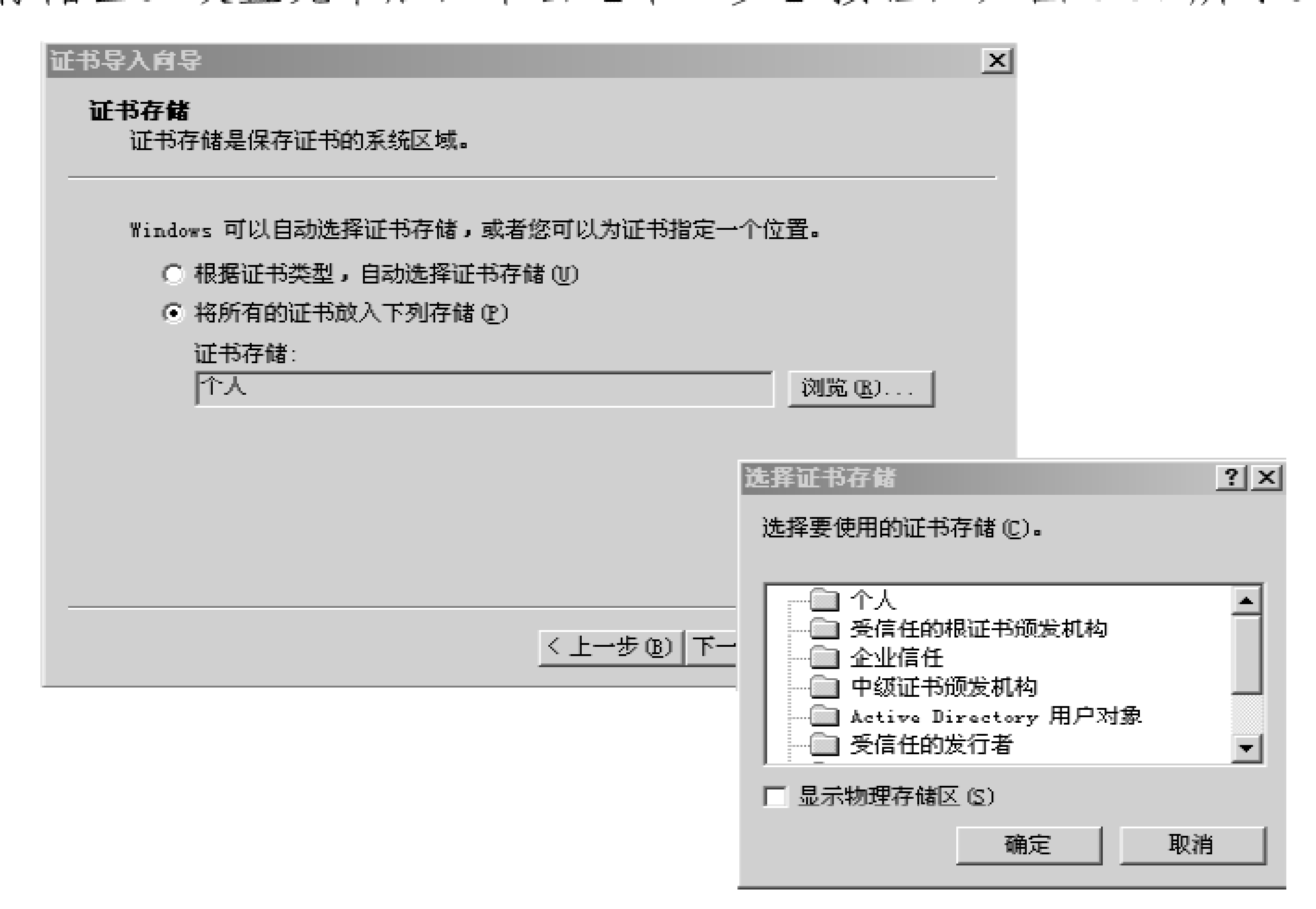


图 6-57　选择证书存放位置

❺ 完成证书导入后，单击【完成】按钮，如图 6-58 所示。



图 6-58　完成证书导入

3. 导出数据证书

导入数据证书就是将证书从使用标准证书存储格式的文件复制到用户账户或计算机账户对应的证书存储区。当下列情况发生时，我们需要导出数据证书。

✧ 备份证书。

✧ 备份证书及其关联的私钥。

✧ 复制证书以便在另一台计算机上使用。

✧ 从证书所有者当前的计算机上删除证书及相关私钥，以便安装在另一台计算机上。

下面简要地介绍一下导出数据证书的操作步骤。

❶ 在【证书颁发机构】管理控制台窗口的控制树中，选择【个人】→【证书】，在右窗格中选择相应的证书并右击，在弹出的快捷菜单中选择【所有任务】→【导出】命令，打开证书导出向导，如图 6-59 所示。



图 6-59　打开证书导出向导

❷ 在弹出的【证书导出向导】对话框中，单击【下一步】按钮，如图 6-60 所示。

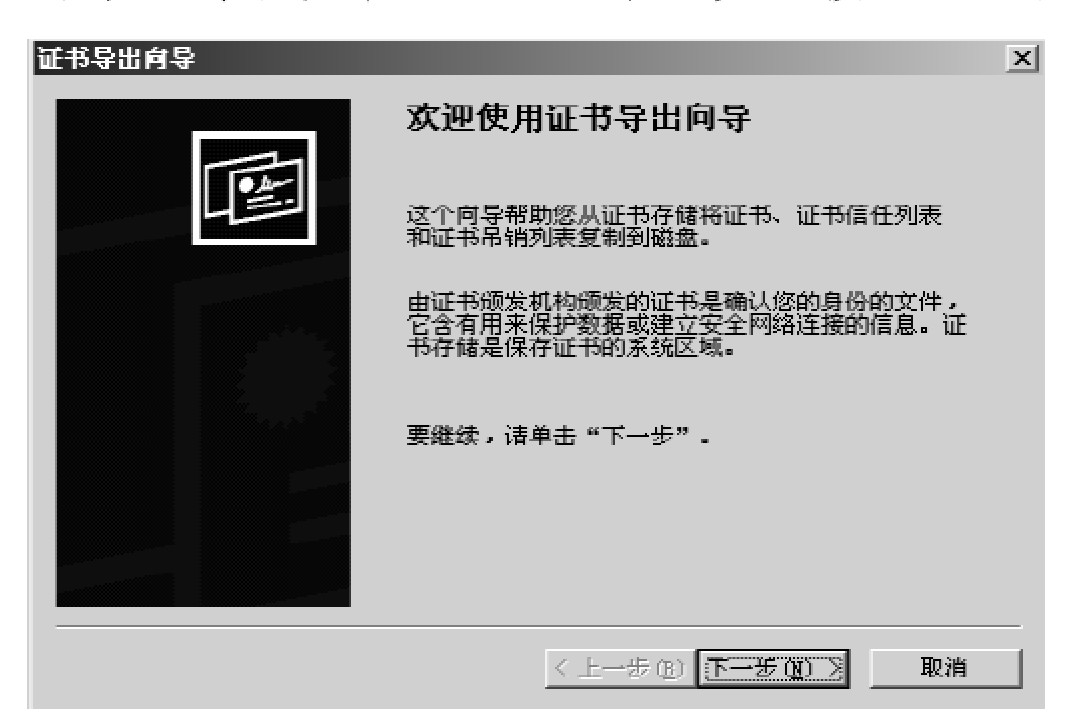


图 6-60　【证书导出向导】对话框

❸ 在【导出私钥】向导页中，选择导出私钥是否受密码保护。设置完毕后，单击【下一步】按钮，如图 6-61 所示。



图 6-61　选择导出私钥是否受密码保护

❹ 如果第❸步选择是导出私钥，则导出文件格式只能选择 PKCS #12，如图 6-62 所示。

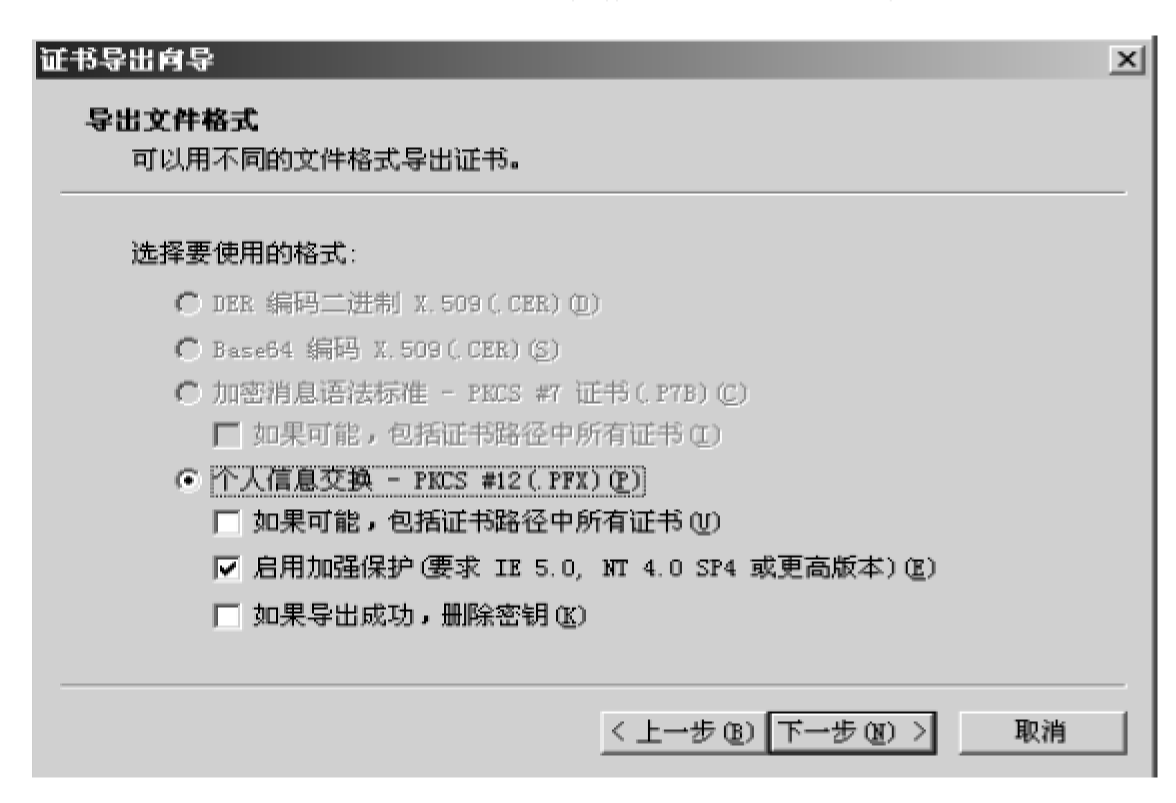


图 6-62　选择私钥带密码保护

❺ 如果第❸步选择不要导出私钥，可以选择 PKCS #7、BASE64 或者 DER 格式，如图 6-63 所示。

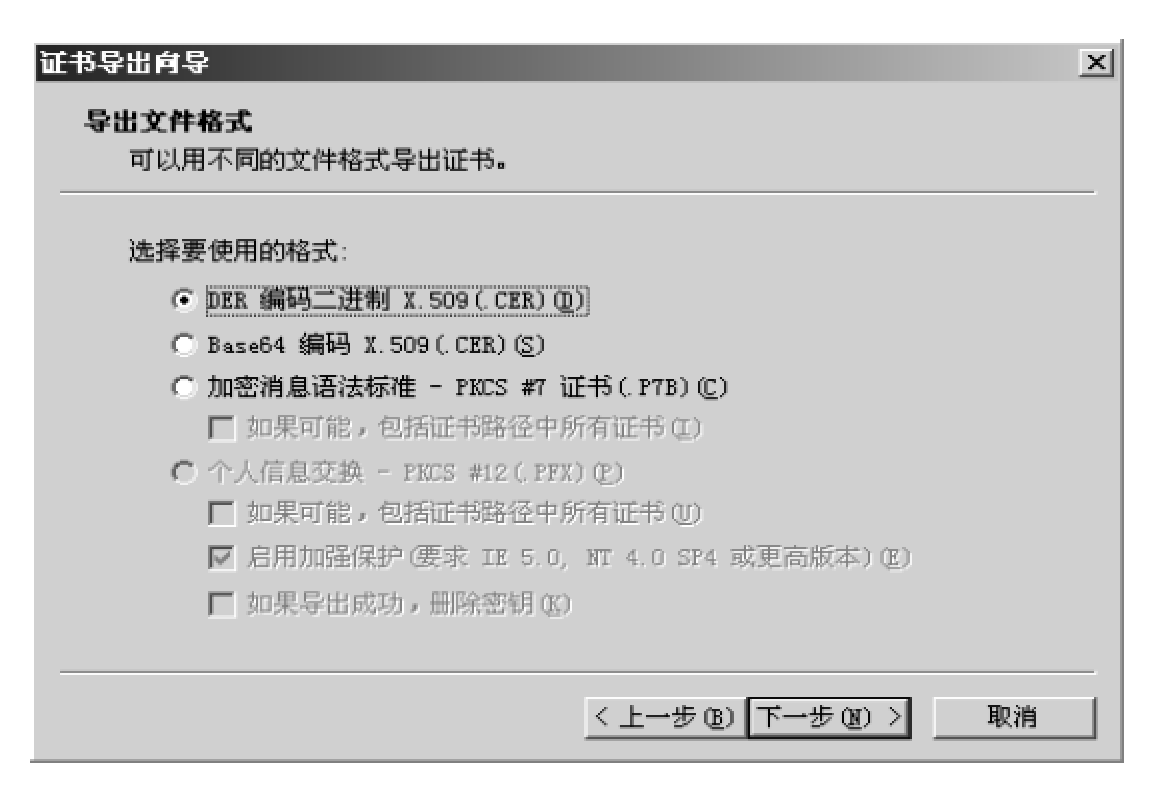


图 6-63　选择私钥不带密码保护

❻ 如果第❸步选择导出私钥受密码保护，则需要输入密码，并单击【下一步】按钮，如图 6-64 所示。



图 6-64　输入密码

❼ 在【要导出的文件】向导页中，选择输出的文件名，并单击【下一步】按钮，如图 6-65 所示。



图 6-65　指定输出的文件名

❽ 完成证书导出后，单击【完成】按钮，如图 6-66 所示。

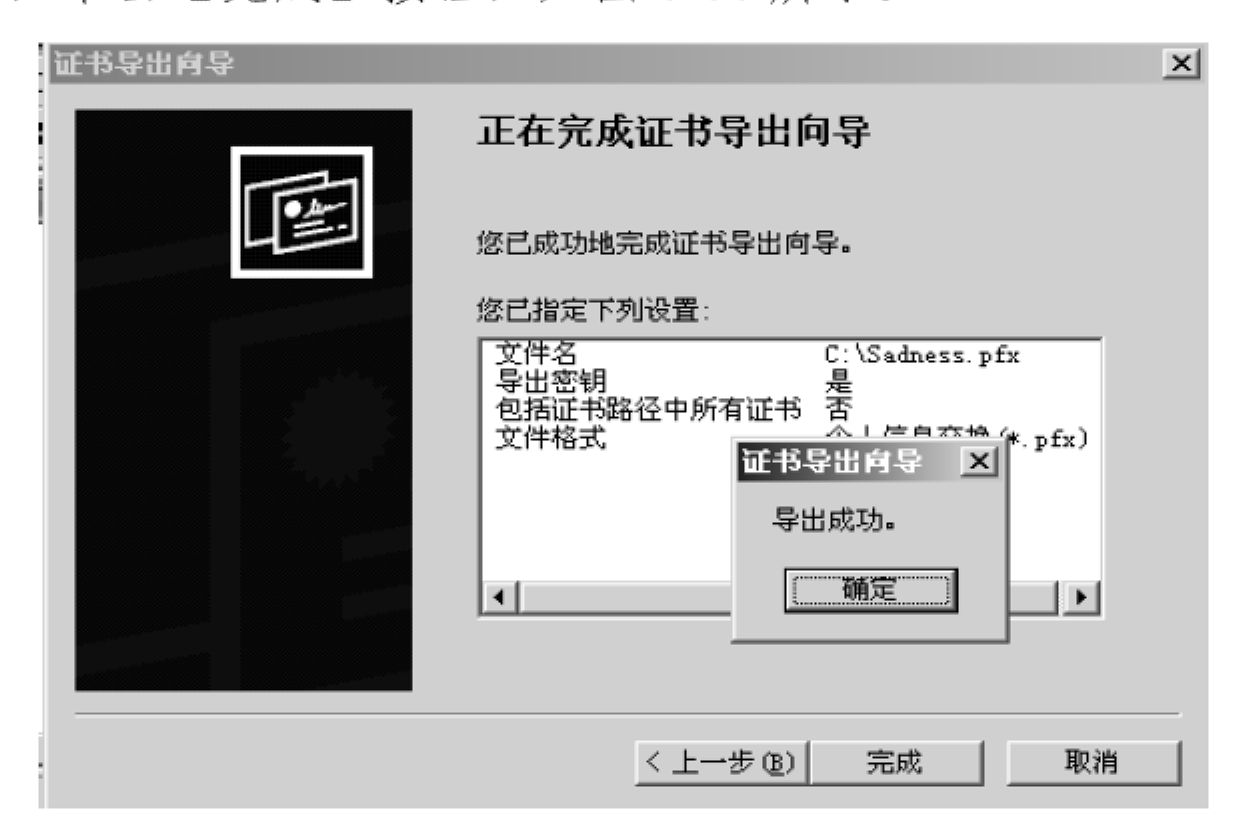


图 6-66　完成导出

6.2　AAA 体系结构

应用实例导航：Sadness 公司部署基于 AAA 身份认证

※场景呈现

Sadness 公司随着业务的发展，网络规模逐渐扩大。可惜每次网络升级都由不同的运营商完成，所有网络设备的密码则不尽相同。这给网络管理带来了极大的不便，每当网络管理部门有人离职的时候，则需要对原有设备的所有密码进行重新设置，这对于拥有上千台网络设备的 Sadness 公司而言，相当困难。同时由于密码修改不及时，还会导致很多攻击事

件的发生。

当 Sadness 聘请 Jam 担任网络安全管理员后，Jam 开始在 Sadness 公司内部部署 AAA 服务，并根据不同的用户分配了不同的权限。通过记账服务也保证了 Jam 日后可以对员工的每一项行为进行审计。

※技术要领

(1) AAA 体系结构；
(2) 在交换机或路由器中配置身份认证；
(3) 在交换机或路由器中配置授权；
(4) 在交换机或路由器中配置记账。

6.2.1　AAA 概述

AAA 指的是认证(Authentication)、授权(Authorization)和统计记账(Accounting)。自网络诞生以来，认证、授权以及记账体制(AAA)就成为其运营的基础。网络中各类资源的使用，需要由认证、授权和记账进行管理，而 AAA 的发展与变迁自始至终都吸引着运营商的目光。对于一个商业系统来说，认证是至关重要的，只有确认了用户的身份，才能知道所提供的服务应该向谁收费，同时也能防止非法用户(黑客)对网络进行破坏。在确认用户身份后，根据用户开户时所申请的服务类别，系统可以授予客户相应的权限。最后，在用户使用系统资源时，需要有相应的设备来统计用户对资源的占用情况，据此向客户收取相应的费用。

其中，认证是指用户在使用网络系统中的资源时对用户身份的确认。这一过程通过与用户的交互获得身份信息(诸如，用户名-口令组合、生物特征获得等)，然后提交给认证服务器；后者对身份信息与存储在数据库里的用户信息进行核对处理，然后根据处理结果确认用户身份是否正确。例如，GSM(全球通)移动通信系统能够识别其网络内网络终端设备的标志和用户标志。授权网络系统授权用户以特定的方式使用其资源，这一过程指定了被认证的用户在接入网络后能够使用的业务和拥有的权限，如授予的 IP 地址等。仍以 GSM 移动通信系统为例，认证通过的合法用户，其业务权限(是否开通国际电话主叫业务等)是用户和运营商在事前已经协议确立的。统计记账网络系统收集、记录用户对网络资源的使用，以便向用户收取资源使用费用，或者用于审计等目的。以互联网接入业务供应商 ISP 为例，用户的网络接入使用情况可以按流量或者时间被准确记录下来。

AAA 是一种体系结构，用来以一致的方式配置一组三种独立的安全功能。它提供了模块化的执行方式来进行身份认证、授权和记账统计服务，如图 6-67 所示。

AAA 体系结构的优点如下。

✧ 通常需要一台或一组服务器(称为安全服务器)来存储用户名和密码，而不用在每台路由器上配置和更新。
✧ 支持 TACACS+、RADIUS 和 Kerberos 标准安全协议。
✧ 允许配置多个备用系统，例如，先访问安全服务器，如果报错，再查看本地数据库。
✧ 用户名和密码不以明文形式出现。

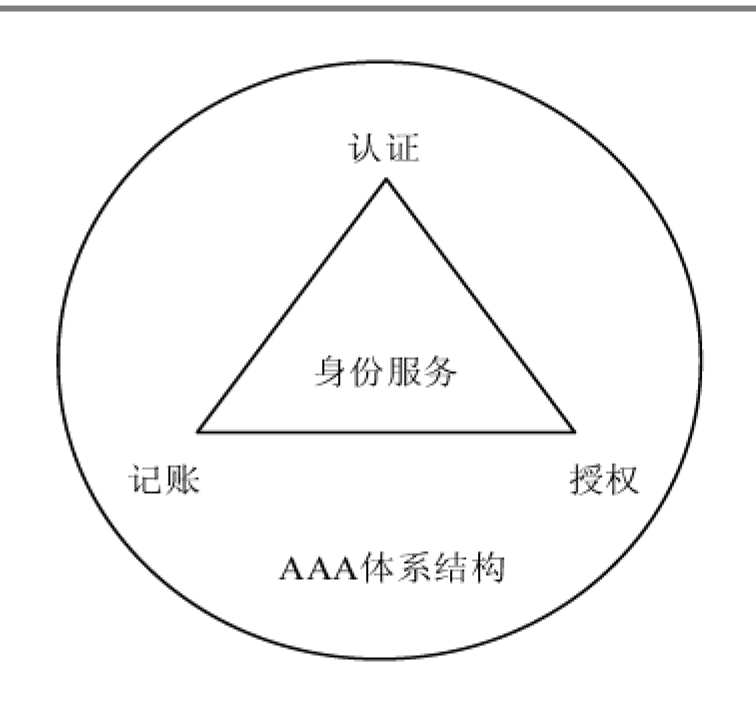


图 6-67 AAA 体系结构

1. 身份认证

身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法，包括登录和口令、询问和应答、消息支持和加密。通过定义一个身份认证方法的命名列表并将其应用于各个接口来配置协议。身份认证的协议支持 TACACS+、 RADIUS、Kerberos 标准安全协议。

TACACS+是 Cisco 公司的私有协议，而 RADIUS 是一种开放标准，两者的不同之处主要在于 TACACS+分离了认证、授权和记账的功能，另外，TACACS+使用 TCP 协议，而 RADIUS 使用 UDP 协议。RADIUS 是目前支持无线验证协议的唯一安全协议。

RADIUS 是一个分布式客户/服务器系统，典型的 RADIUS 客户端是 NAS(网络接入服务器)，而服务器端通常是一个运行在 UNIX 或者 Windows 系统上的守护进程。客户端将用户信息传递给指定的 RADIUS 服务器，服务器负责接收用户连接请求、验证用户是否合法，并将向用户提供的服务信息返回给客户端。

我们可以定义一个方法列表使用不同的协议来对用户身份进行认证。例如，在图 6-68 中，管理员可以定义一个方法列表，首先从 RADIUS 1 中获取身份认证信息，然后是 RADIUS 2、TACACS+ 1、TACACS+ 2。假如用户先在 RADIUS 1 上认证通过，则可以访问内部网络，如果 RADIUS 1 失败，则返回 Error 认证失败消息，按顺序验证 RADIUS 2、TACACS+ 1、TACACS+ 2。全部认证失败后，则拒绝通过。当然在其中任何一步如果认证失败，则直接返回认证失败消息，终止对话。

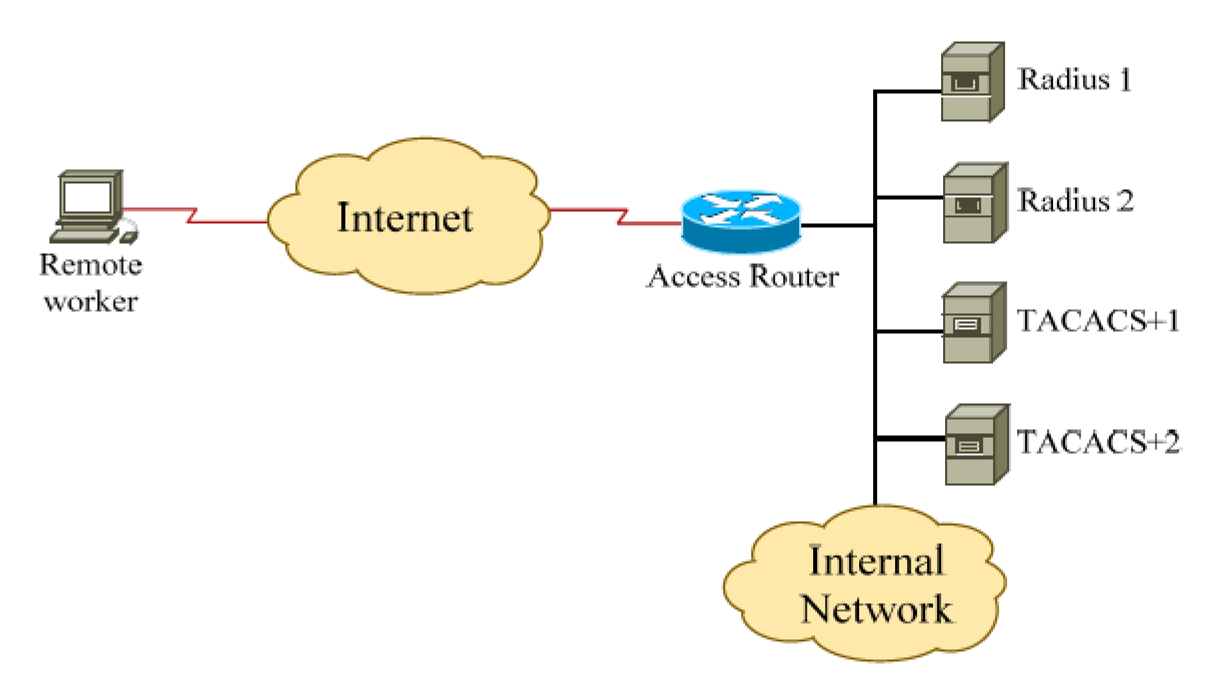


图 6-68 身份认证

2. 授权

授权是为远程访问控制提供方法，包括一次性授权或者每种服务的授权等，单个用户的统计列表和概述，以及用户组支持协议的授权等。AAA 授权通过一系列属性来作用于用户，这些属性描述了用户被授权执行的操作。系统将这些属性同包含在数据库中的指定用户信息比较，将结果返回给 AAA，从而确定该用户实际拥有的权限和所受的约束。数据库通常存放在 RADIUS 或者 TACACS+安全服务器上，它们通过将用户与属性值(AV)相关联来给予用户相应的权限。所有的授权方法都必须通过 AAA 定义。

3. 记账

记账是提供收集和发送用于计费、审计、制作报表的安全服务器信息的方法。统计的内容包括用户身份、开始和结束时间、所执行命令、分组数和字节数等。记账使得管理员可以容易地记录用户正在访问的服务以及它们占用的网络资源量。当 AAA 记账激活时，网络服务器便开始以统计记录的形式向 RADIUS 或者 TACACS+服务器发送用户的活动状态等信息。每个统计记录均被储存，它们将被用于对客户记账或者对员工操作进行审计等。

当然，AAA 在支持 TACACS+、RADIUS、Kerberos 标准安全协议时也遇到以下一些问题。

- ✧ Kerberos 不支持 AAA 中的授权和记账。
- ✧ TACACS+，是 Cisco 专有协议运行于 TCP 上，能对有效负载进行加密，能控制用户权限等级，可将认证和授权分开，因此可使用 TACACS+进行授权和记账，而用其他方法进行认证。
- ✧ RADIUS 运行于 UDP 上，只对密码进行加密，不能控制用户权限等级，不可将验证和授权分开。

目前，业界用的最为广泛的协议为 RADIUS，并且 RADIUS 可以在 Windows 上由微软 IAS、Cisco ACS 或 Linux 的 RADIUS 服务提供，它们的详细配置方法将在 6.3 节中介绍。

6.2.2　配置 AAA 身份认证

AAA 身份认证通常有登录身份认证、PPP(点对点协议)身份认证、NASI(异步服务接口)身份认证、ARA(Appletalk 远程访问协议)身份认证等 4 种方式。通常我们所使用的网络中 NASI 和 ARA 需求很少，因此我们将着重讲解 AAA 配置登录身份认证和 PPP 身份认证的方法。

1. AAA 配置登录身份认证

AAA 安全服务使得大量的登录身份认证变得容易，再也不会因为员工离职而大批量更改密码，只需在安全认证服务器上删除该员工账号即可。AAA 配置登录认证的方式较为简单，均可使用 aaa authentication login 命令启动。

AAA 配置登录身份认证时，可以采用本地口令进行身份认证，也可以采用 RADIUS 进行登录身份认证，下面分别介绍这两种认证的配置方法。

1)　使用本地口令进行身份认证

❶ 在交换机或路由器的全局配置模式下，启用 AAA。

```
Router(config)#aaa new-model
```

❷ 由于使用本地口令进行身份认证，接着需要定义本地口令数据库、分配用户权限、启用密码加密服务，使得配置文件中密码不以明码方式储存。

```
Router(config)#username cisco password cisco
Router(config)#username cisco privilege 15
Router(config)#service password-encryption
Router(config)#username cisco access-class 1
Router(config)#username cisco autocommand show run
```

❸ 创建 AAA 认证方法列表。

```
Router(config)#aaa authentication login default line
```

❹ 如果使用线路口令进行身份认证，首先需要配置线路口令，再启用用户登录功能。

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#login authentication {default | list name}
```

❺ 配置使用 enable 口令进行登录身份认证。

```
Router(config)#enable secret cisco
Router(config)#aaa authentication login default enable
```

2) 使用 RADIUS 进行身份认证

❶ 在交换机或路由器的全局配置模式下，启用 AAA。

```
Router(config)#aaa new-model
```

❷ 由于使用 RADIUS 进行登录身份认证，首先需要在路由器上指定相应的 RADIUS 服务器或者 RADIUS 服务器组。如果网络中只有一台 RADIUS 服务器，则指定方法如下。

```
Router(config)#radius-server host 10.0.0.2 auth_port 1645 acct-port 1646
```

如果网络中只有多台 RADIUS 服务器，需要指定 RADIUS 服务器组，方法如下。

```
Router(config)#aaa group server radius sadnessradius
Router(config-sg-radius)#server 10.0.0.1
Router(config-sg-radius)#server 10.0.0.2
Router(config-sg-radius)#server 10.0.0.3
```

❸ 将服务器或服务器组映射到 AAA 认证方法中。

```
Router(config)#aaa authentication login default radius
Router(config)#aaa authentication login default group sadnessradius
```

❹ 有时候网络设备出现故障进行维修时，无法连接到 RADIUS 服务器，则在使用 RADIUS 服务器时，需要在 RADIUS 认证后面加入 local 或者 enable 或者 line 的认证方式，以方便维修人员能够本地连接上设备。

```
Router(config)#aaa authentication login default radius local
```

❺ 当然，有时候网络管理员也可以选择使用身份本地覆盖功能，身份本地覆盖功能允许 Cisco IOS 在尝试其他认证方式前，优先使用本地认证。

```
Router(config)#aaa authentication local-override
```

 与使用本地口令进行身份认证一样，将身份认证方法列表使用在相应的接口上或使用 enable 口令认证。

2. 利用 AAA 配置 PPP 身份认证

很多时候，网络故障发生在深夜，管理员通常需要在家中通过 ISDN(综合业务数字网)或者传统电话(PSTN)远程连接到网络中进行网络配置和故障处理，此时通常使用的协议是 PPP。

1)　PPP 协议简介

PPP(Point-to-Point Protocol，点对点协议)是为在同等单元之间传输数据包的简单链路设计的链路层协议。这种链路提供全双工操作，并按照顺序传递数据包。设计目的主要是用来通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种共通的解决方案。目前大多数模拟拨号连接都采用 PPP 作为数据链路协议。

PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。PPP 和串行线路因特网协议(SLIP)常常使人混淆，PPP 在很多方面都优于 SLIP，其中最重要的一点是它的可扩展性，SLIP 仅仅支持 IP 协议，而 PPP 支持 IP、IPX 以及 AppleTalk 等多协议。PPP 由封装方法(HDLC)、链路控制协议(Link Control Protocol，LCP)和网络控制协议(Network Control Protocol，NCP) 3 个组件组成。

2)　PPP 链路建立过程

一个典型的 PPP 链路建立过程分为创建阶段、认证阶段和网络协商阶段 3 个阶段。

- ✧ 第 1 阶段——创建 PPP 链路。LCP 负责创建链路。在这个阶段，将对基本的通信方式进行选择。链路两端设备通过 LCP(链路控制协议)向对方发送配置信息包。一旦一个配置成功信息包被发送且被接收，就完成了交换，进入了 LCP 开启状态。应当注意，在链路创建阶段，只是对认证协议进行选择，用户认证将在第 2 阶段实现。
- ✧ 第 2 阶段——用户验证。在这个阶段，客户端会将自己的身份发送给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。在认证完成之前，禁止从认证阶段前进到网络层协议阶段。如果认证失败，认证者应该跃迁到链路终止阶段。在这一阶段里，只有链路控制协议、认证协议和链路质量监视协议的信息包是被允许的。在该阶段里接收到的其他的数据包必须被静静地丢弃。最常用的认证协议有口令验证协议(PAP)和挑战-握手验证协议(CHAP)。
- ✧ 第 3 阶段——调用网络层协议。认证阶段完成之后，PPP 将调用在链路创建阶段(第 1 阶段)选定的各种网络控制协议(NCP)。选定的 NCP 用于解决 PPP 链路之上的高层协议问题。例如，在该阶段 IP 控制协议(IPCP)可以向拨入用户分配动态地址。这样，经过 3 个阶段以后，一条完整的 PPP 链路就建立起来了。

3)　PPP 认证

PPP 认证可以采用口令认证协议(Password Authentication Protocol，PAP)和挑战-握手验证协议(Challenge-Handshake Authentication Protocol，CHAP)两种认证方式。

- ✧ PAP 协议：PAP 是一种简单的明文验证方式。NAS(网络接入服务器，Network

Access Server)要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障措施。

✧ CHAP 协议：CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令，其中包括会话 ID 和一个任意生成的挑战字串。远程客户必须使用 MD5 单向哈希算法返回用户名和加密的挑战口令，会话 ID 以及用户口令，其中用户名以非哈希方式发送。CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字串来防止受到再现攻击。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第三方冒充远程客户进行攻击。

4) 利用 AAA 配置 PPP 身份认证

AAA 配置 PPP 身份认证与 AAA 配置登录身份认证相似，既可以采用本地口令进行身份认证，也可以采用 RADIUS 进行身份认证。下面分别介绍这两种认证的配置方法。

1) 使用本地口令进行身份认证

❶ 在全局配置模式下，启用 AAA。

```
Router(config)#aaa new-model
```

❷ 如果使用本地口令进行身份认证，需要定义本地口令数据库。

```
Router(config)#username cisco password cisco
```

❸ 分配用户权限并启用密码加密服务，使得配置文件中的密码不以明码方式储存。

```
Router(config)#username cisco privilege 15
Router(config)#service password-encryption
```

❹ 当然还可以使用一些可选属性，例如使用访问控制列表控制登录地址，或者设置登录后自动执行的命令等。

```
Router(config)#username cisco access-class 1
Router(config)#username cisco autocommand show run
```

❺ 完成如上配置后，创建 AAA 认证方法。

```
Router(config)#aaa authentication ppp default local
```

❻ 将配置的身份认证方法列表并使用在相应的接口上。

```
Router(config)#interface Serial1/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authenticaition {pap | chap | chap pap | pap chap}
{default | listname}
```

2) 使用 RADIUS 进行身份认证

❶ 在全局配置模式下，启用 AAA。

```
Router(config)#aaa new-model
```

❷ 由于采用 RADIUS 进行身份认证，首先还需要在路由器上指定相应的 RADIUS 服务器或者 RADIUS 服务器组。指定单个 RADIUS 服务器的方法如下。

```
Router(config)#radius-server host 10.0.0.2 auth_port 1645 acct-port 1646
```

指定 RADIUS 服务器组的方法如下。

```
Router(config)#aaa group server radius sadnessradius
Router(config-sg-radius)#server 10.0.0.1
Router(config-sg-radius)#server 10.0.0.2
Router(config-sg-radius)#server 10.0.0.3
```

❸ 将服务器或服务器组映射到 AAA 认证方法中。

```
Router(config)#aaa authentication ppp default radius
Router(config)#aaa authentication ppp default group sadnessradius
```

❹ 如果有时候网络设备出现故障进行维修，无法连接到 RADIUS 服务器，则在使用 RADIUS 服务器的时候，我们通常还会在方法列表中 RADIUS 认证的后面加入 local 或者 enable 或者 line 的认证方式，以方便维修人员能够本地连接上设备。

```
Router(config)#aaa authentication ppp default radius local
```

❺ 将配置的身份认证方法列表使用在相应的接口上。

3. 使用双重身份认证

双重身份认证为 PPP 会话提供了额外的身份认证。按照前面的配置，PPP 仅使用单个身份认证方法(PAP 或者 CHAP)进行认证。而双重身份认证是指当用户通过 PPP 认证后，还将通过第 2 阶段的认证。

第 2 阶段认证需要一条用户知道单位存储在用户的远端主机上的口令，因此第 2 阶段身份认证针对的是用户本身，并且第 2 阶段认证可以使用一次性口令等 CHAP 不支持的方式，可以很好地提高系统的安全性。

例如，Jam 通过 PPP 建立远程站点到公司网络设备的链接后，即便是通过了认证，他也需要 telnet 到网络访问服务器，进行身份认证，然后 Jam 必须输入 access-profile 命令用于 AAA 重新授权。即便是配置了 autocommand access-profile，Jam 也需要 telnet 到本地主机并登录才能完成双重身份认证。关于授权将在 6.2.3 节详细介绍。

4. 使用 AAA 特权保护

一旦攻击者拥有路由器特权模式密码，将可以直接修改路由器的所有配置，其后果是难以想像的，因此我们有必要采用一定的方式来对特权模式进行保护，其配置方法如下。

```
Router(config)#aaa authentication enable default method1 [method2…]
```

点评与拓展： Jam 通过配置 AAA 身份认证使得 Sadness 公司在网络管理员离职后不需要大量更改服务器密码，仅需要 Jam 通过 RADIUS 服务器删除该员工账号即可。新的员工加入公司，也只需要添加一个新的 RADIUS 账号。路由器等设备的本地账号仅能作为网络管理部门负责人 Jam 独自掌握，这样设备的安全性获得了很大的提高。

6.2.3 配置 AAA 授权

AAA 授权能让管理员限制用户可以使用的服务，针对 Sadness 公司不同部门的网络管理员，Jam 可以为他们选择不同的权限。完成 AAA 授权配置后，用户只能被允许使用其用户配置文件中所允许的服务。

❶ 在全局配置模式下，启用 AAA。

```
Router(config)#aaa new-model
```

❷ 创建授权方法。

```
Router(config)#aaa authentication login default group radius
Router(config)#aaa authentication ppp default if-needed group radius
Router(config)#aaa authorization exec default group radius
Router(config)#aaa   authorization   network   default   group   radius
if-authenticated
```

❸ 通过 ACL 配置用户其访问权限。

```
Router(config)#access-list 110 permit tcp any any eq telnet
Router(config)#access-list 110 permit tcp any any eq ftp
Router(config)#access-list 110 permit tcp any any eq ftp-data
Router(config)#access-list 110 deny tcp any any
```

❹ 需要再配置 RADIUS 服务器，引用上面的配置的 ACL 110。下面的例子是在 Cisco ACS 中配置的例子。

```
<CiscoACS>$/opt/ciscosecure/CLI/AddProfile -p 9900 -u Jam -pw pap, cisco -a
'radius=Cisco{\nreply_attributes={\n6=2\n7=1\n9,1="ip:inacl=110"}\n}\n'
```

❺ 下面的配置是 Cisco ACS 验证 RADIUS 服务器的配置文件的片段。

```
<CiscoACS>$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u rad_dial
User Profile Information
user = Jam {
profile_id = 62
profile_cycle = 1
password = pap "********"
radius=Cisco {
reply_attributes= {
6=2
7=1
9, 1="ip:inacl=110"
}
}
}
```

❻ 将配置的身份认证方法列表使用在相应的接口上。

```
Router(config)#line vty 0 4
Router(config-line)# authorization commands 0 default
```

6.2.4 配置 AAA 记账

AAA 记账是提供收集和发送用于记账、审计、制作报表的安全服务器信息的方法。记账的内容包括用户身份、开始和结束时间、所执行命令、分组数和字节数等。记账使得管

理员可以简单地记录用户正在访问的服务以及它们占用的网络资源量。当 AAA 记账激活时，网络服务器便开始以统计记录的形式向 RADIUS 或者 TACACS+服务器发送用户的活动状态等信息。每个统计记录均被储存，它们将被用于对客户计费或者对员工操作进行审计等。AAA 记账包括如下几个组件。

- ✧ Network：提供所有 pppsliparap 会话信息，包括数据包数和字节数。
- ✧ Connection：提供从网络中发起的所有外出连接(例如 telnet、andrlogin)的信息。
- ✧ EXEC：提供接入服务器上的用户 EXEC 会话的信息，包括用户名、日期、起始和结束时间、接入服务器 IP、主叫方电话等。
- ✧ System：提供所有的系统级事件。
- ✧ Commands：提供在网络接入服务器上执行的特定权限级别的 EXEC 外壳。
- ✧ 资源统计：提供了用户身份验证的呼叫的起始和终止记录。

根据审计目的不同，配置方法也不相同。下面简要地介绍对用户的行为进行审计的配置方法。

❶ 若要对用户登录进行审计，可执行如下命令。

```
Router(config)# aaa accounting exec default start-stop group radius
```

❷ 若要对用户所用命令进行审计，可执行如下命令。

```
Router(config)#aaa accounting commands 1 default start-stop group radius
Router(config)#aaa accounting commands 15 default start-stop group radius
```

❸ 若要在线路上应用审计，可执行如下命令。

```
Router(config)# line vty 0 4
Router(config-line)# accounting commands 1 default
Router(config-line)# accounting commands 15 default
Router(config-line)# accounting exec default #
```

📖**点评与拓展：**Jam 通过配置授权和记账给不同的网管员赋予了不同的权限，并且 Jam 可以轻易地从记账报告中查询网管员的登录是否合理，所使用的命令是否安全等。通过 AAA 的实施，Sadness 公司网络设备的管理和维护变得异常方便。AAA 的配置在很大程度上依赖 RADIUS 服务器，在 6.3 节我们将详细介绍 RADIUS 服务器的安装和配置。

6.3　配置 RADIUS 服务器

6.3.1　RADIUS 简介

1. RADIUS 简介

RADIUS(Remote Authentication Dial In User Service，远程认证拨号用户服务) 是 RFC 2865 和 RFC 2866 中描述的业界标准协议，用于提供身份验证、授权和记账统计服务。RADIUS 客户端是网络访问服务器(Network Access Server，NAS)，它通常是一台路由器、交换机、拨号服务器、VPN 服务器或无线访问点，它以 RADIUS 消息的形式向 RADIUS

服务器发送用户凭据和连接参数信息。RADIUS 服务器对 RADIUS 客户端请求进行身份验证和授权，并发回 RADIUS 消息响应。RADIUS 客户端也向 RADIUS 服务器发送 RADIUS 记账统计消息，如图 6-69 所示。另外，RADIUS 标准支持使用 RADIUS 代理，它是在启用 RADIUS 的计算机之间转发 RADIUS 消息的计算机。

RADIUS 消息作为用户数据报协议 (UDP) 消息被发送。UDP 端口 1812 用于发送 RADIUS 身份验证消息，UDP 端口 1813 用于发送 RADIUS 记账统计消息。有些网络访问服务器可能会使用 UDP 端口 1645 发送 RADIUS 身份验证消息，而使用 UDP 端口 1646 发送 RADIUS 记账统计消息。

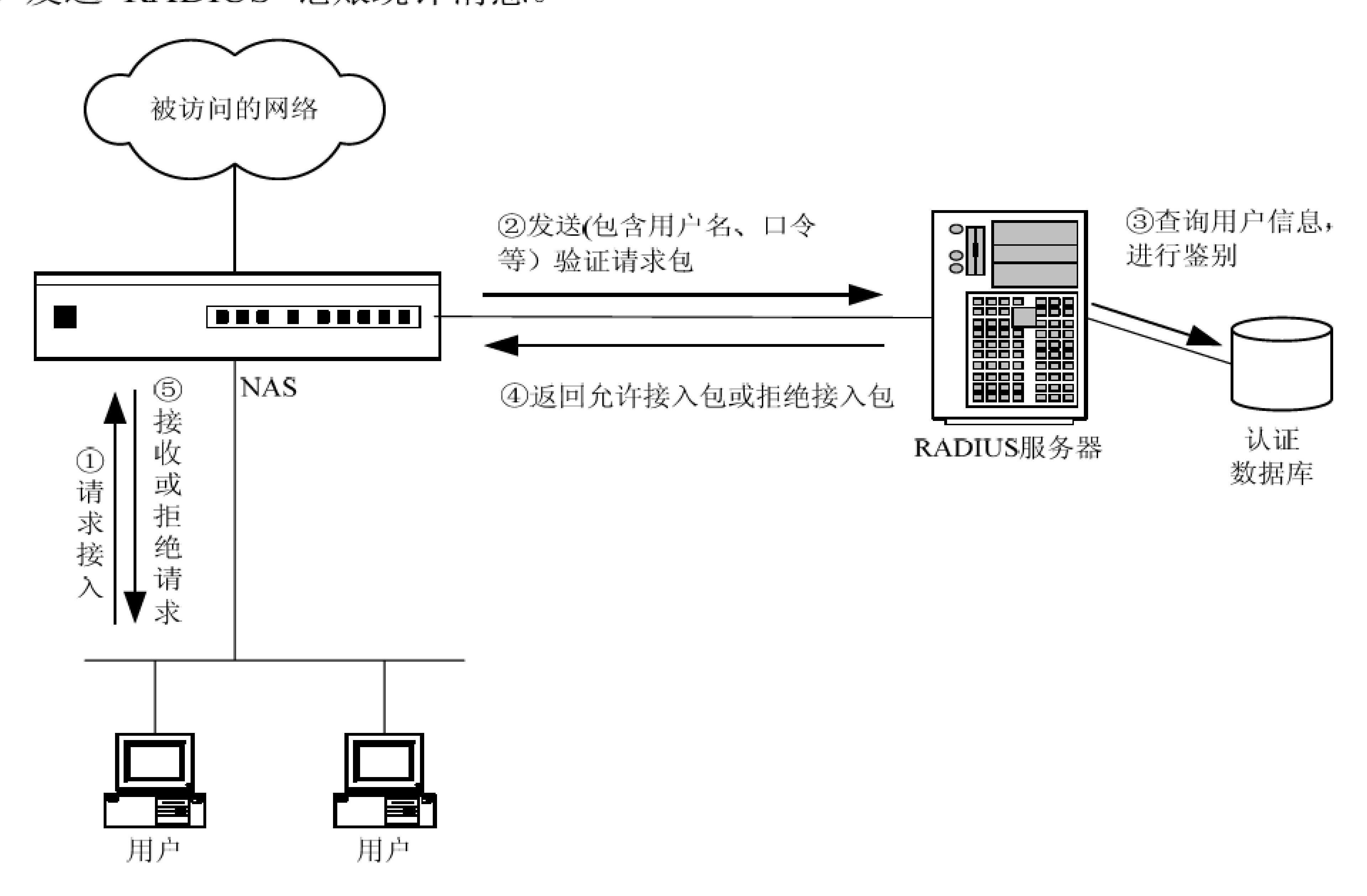


图 6-69　RADIUS 连接示意图

2. RADIUS 消息类型

RFC2865 和 RFC2866 定义了以下 RADIUS 消息类型。

- ✧ 接入-请求(Access-Request)：由 RADIUS 客户端发送请求对连接尝试进行身份验证和授权。
- ✧ 接入-接收(Access-Accept)：由 RADIUS 服务器发送，以响应“接入-请求”消息，此消息通知 RADIUS 客户端已对连接尝试进行身份验证和授权。
- ✧ 接入-拒绝(Access-Reject)：由 RADIUS 服务器发送，以响应“接入-请求”消息，此消息通知 RADIUS 客户端连接尝试被拒绝，如果凭据未被验证或连接尝试未被授权，RADIUS 服务器将发送此消息。
- ✧ 接入-质询(Access-Challenge)：由 RADIUS 服务器发送，以响应“接入-请求”消息，此消息是对需要响应的 RADIUS 客户端的质询。
- ✧ 记账统计-请求(Accounting-Request)：由 RADIUS 客户端发送，为接受的连接指定记账统计信息。

- ✧ 记账统计-响应(Accounting-Response)：由 RADIUS 服务器发送，以响应“记账统计-请求”消息，此消息确认对记账统计请求消息的成功接受和处理。

3. RADIUS 协议的主要特点

RADIUS 协议有以下几项主要特点。

- ✧ 客户/服务器模式：网络接入服务器作为 RADIUS 的客户端，负责将用户信息传递给指定的 RADIUS 服务器，然后根据返回信息进行操作。RADIUS 服务器负责接收用户连接请求，认证用户后，返回所有必要的配置信息以便客户端为用户提供服务。RADIUS 服务器可以作为其他 RADIUS 服务器或认证服务器的代理。
- ✧ 网络安全：客户端与 RADIUS 记账统计服务器之间的通信是通过共享密钥来鉴别的，这个共享密钥不会通过网络传送。此外，任何用户口令在客户机和 RADIUS 服务器间发送时都需要进行加密过程，以避免有人通过嗅探非安全网络得到用户密码。
- ✧ 灵活认证机制：RADIUS 服务器支持多种用户认证方法。当用户提供了用户名和原始口令后，RADIUS 服务器可支持 PPP PAP 或 CHAP、UNIX 登录和其他认证机制。
- ✧ 协议的可扩充性：所有的事务都是由不同长度的“属性-长度-值”三元组构成的。新属性值的加入不会影响到原有协议的执行。

4. RADIUS 的工作过程

RADIUS 协议旨在简化认证流程，其典型认证工作过程如图 6-69 所示，具体如下。

(1) 用户输入用户名、密码等信息到客户端或连接到 NAS。

(2) 客户端或 NAS 产生一个接入-请求报文到 RADIUS 服务器，其中包括用户名、口令、客户端(NAS)ID 和用户访问端口的 ID。口令经过 MD5 算法进行加密。

(3) RADIUS 服务器通过查询认证数据库对用户进行认证。

(4) 若认证成功，RADIUS 服务器向客户端或 NAS 发送允许接入报文，否则发送拒绝接入报文。

(5) 若客户端或 NAS 接收到允许接入报文，则为用户建立连接，对用户进行授权和提供服务；若接收到拒绝接入报文，则拒绝用户的连接请求，结束协商过程。

5. RADIUS 服务

部署 RADIUS 并不困难，有几种途径可以实现，选择哪种途径取决于用户的网络采用的操作系统。如果是 Microsoft 产品，可以使用 Internet 认证服务(Internet Authentication Services，IAS)来部署 RADIUS，其操作重点在于对域的设置。如果使用的是 Linux，则有许多免费的软件包，例如 IC-RADIUS、FreeRADIUS 等。另外，Cisco 也提供 Cisco Secure ACS 服务器用于 TACACS+和 RADIUS 的认证。

下面我们将分为 3 个小节来分别介绍微软 IAS、Cisco Secure ACS 以及 Linux RADIUS 的安装与配置方法。

6.3.2　微软 IAS

一台安装 IAS 的 Windows Server 2003 服务器可以扮演 RADIUS 服务器或 RADIUS 代

理服务器的角色。作为 RADIUS 服务器，IAS 服务器执行多种类型网络访问的集中式连接身份验证、授权和记账统计，这些访问类型包括无线、身份验证交换机、拨号和虚拟专用网(VPN)远程访问以及路由器对路由器连接。作为 RADIUS 代理，IAS 服务器向其他 RADIUS 服务器转发身份验证和记账统计消息。IAS 完成支持 RADIUS 的 Internet 工程任务组(IETF)标准 RFC 2865 和 RFC 2866。

IAS 服务器允许使用各种无线、交换机、远程访问或 VPN 设备，可以将 IAS 服务器与路由和远程访问服务配合使用，对这些用户进行身份验证、授权和记账统计。

如果 IAS 服务器是 Active Directory 域的成员，则 IAS 服务器使用目录服务作为其用户账户数据库，并且是单一登录解决方案的一部分。同一组凭据可用于网络访问控制(对网络进行身份验证和授权访问)，并可以登录到 Active Directory 域。

1. IAS 工作模式

IAS 服务器可以作为 RADIUS 服务器也可以作为 RADIUS 代理服务器。

1) RADIUS 服务器

当 IAS 服务器用作 RADIUS 服务器时，将 Internet 认证服务(IAS)器用作 RADIUS 服务器时，它提供以下功能。

- ✧ RADIUS 客户端发送的所有访问/请求的集中的身份验证和授权服务。IAS 服务器使用域、Active Directory 域或本地“安全账户管理器”(SAM) 来验证进行连接尝试的用户凭据。IAS 服务器使用用户账户和远程访问策略的拨入属性对连接进行授权。
- ✧ RADIUS 客户端发送的所有记账统计请求的集中的记账统计记录服务。记账统计请求存储在本地日志文件中以便进行分析。

图 6-70 显示了作为各种访问客户端的 RADIUS 服务器和 RADIUS 代理的 IAS 服务器。IAS 服务器使用 Active Directory 域，对传入的 RADIUS “接入-请求”消息的用户凭据进行身份验证。

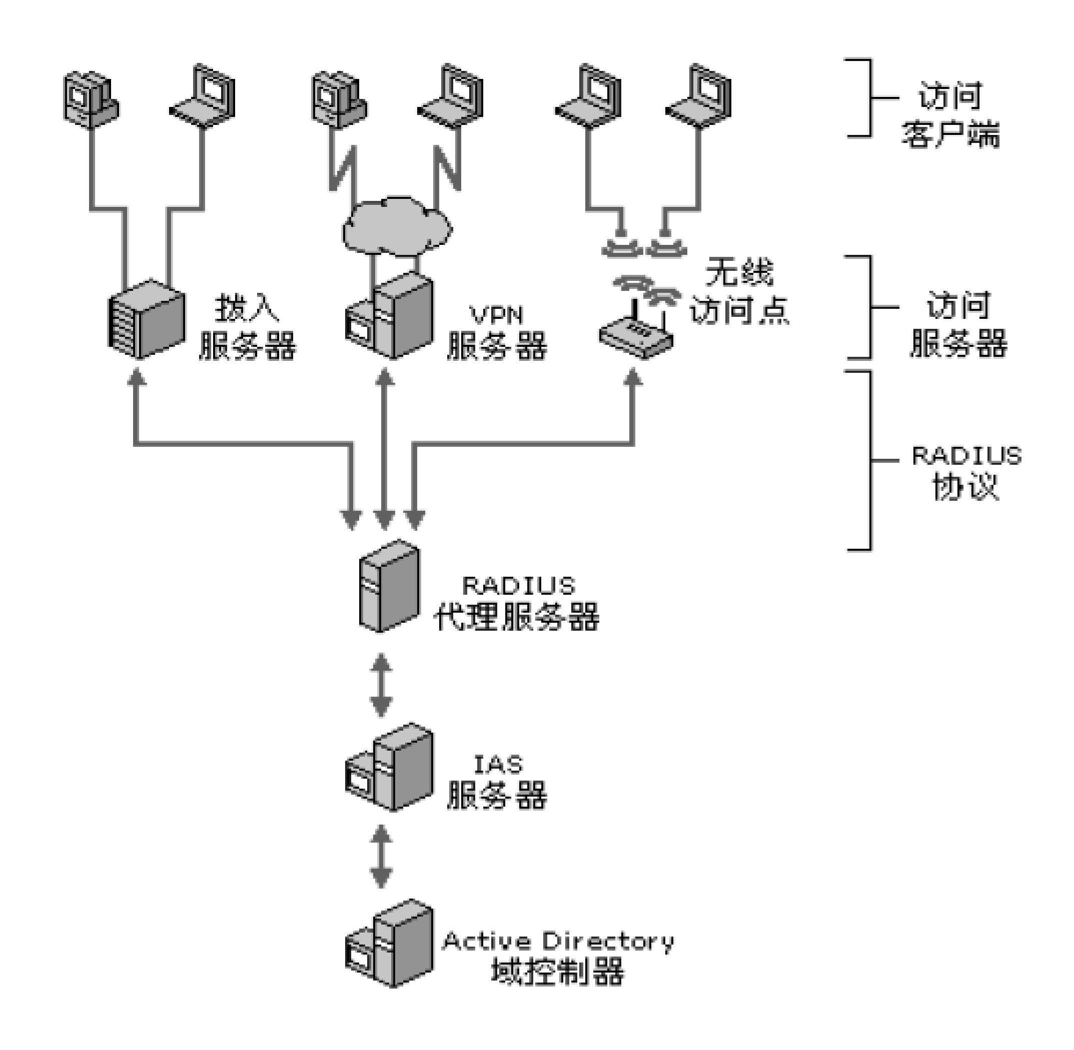


图 6-70　IAS 服务器作为 RADIUS 服务器

RADIUS 消息通过以下方式为网络访问连接提供身份验证、授权和记账统计。

✧ 访问服务器，例如拨号网络访问服务器、VPN 服务器以及无线访问点，接收来自访问客户端的连接请求。
✧ 被配置为使用 RADIUS 作为身份验证、授权和记账统计协议的访问服务器，创建“接入-请求”消息，并将其发送到 IAS 服务器。
✧ IAS 服务器对“接入-请求”消息进行评估。
✧ 如果需要，IAS 服务器将向访问服务器发送“接入-质询”消息，访问服务器处理质询，并向 IAS 服务器发送更新的“接入-请求”。
✧ 通过使用与域控制器的安全连接，可以检查用户凭据，获得用户账户的拨入属性；
✧ 使用用户账户的拨入属性和远程访问策略对连接尝试进行授权。
✧ 如果已对连接尝试进行身份验证和授权，那么 IAS 服务器将向访问服务器发送“接入-接受”消息，如果未对连接尝试进行身份验证或授权，那么 IAS 服务器将向访问服务器发送“接入-拒绝”消息。
✧ 访问服务器完成与访问客户端的连接处理，并向消息登录的 IAS 服务器发送“记账统计-请求”消息。
✧ IAS 服务器向访问服务器发送“记账统计-响应”。

2) RADIUS 代理服务器

IAS 服务器也可以用作 RADIUS 代理服务器，以便提供 RADIUS 客户端和 RADIUS 服务器之间的 RADIUS 消息的路由。用作 RADIUS 代理服务器时，IAS 服务器是 RADIUS 访问消息和记账统计消息流经的中心切换点或路由点。

图 6-71 显示了作为 RADIUS 客户端(访问服务器)和 RADIUS 服务器(或另一个 RADIUS 代理)之间的 RADIUS 代理的 IAS 服务器。

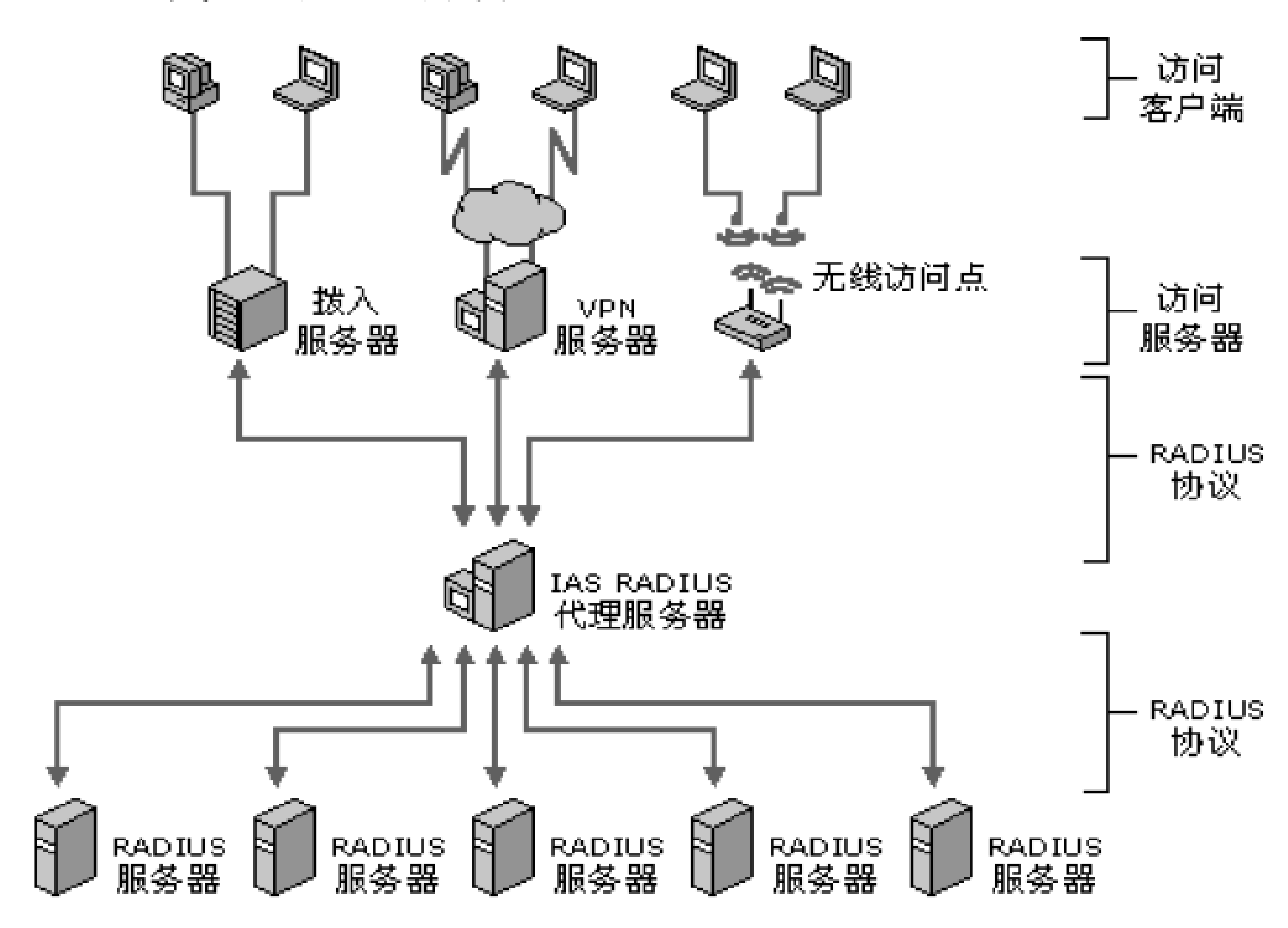


图 6-71　IAS 服务器作为 RADIUS 代理服务器

当 IAS 服务器用作 RADIUS 客户端和 RADIUS 服务器之间的 RADIUS 代理时，将通过以下方式转发网络连接尝试的 RADIUS 消息。

- ✧ 访问服务器(例如拨号网络访问服务器、VPN 服务器以及无线访问点)接收来自访问客户端的连接请求。
- ✧ 被配置为将 RADIUS 用作身份验证、授权和记账统计协议的访问服务器，将会创建访问请求消息，并将其发送到正被用作 IAS RADIUS 代理的 IAS 服务器。
- ✧ IAS RADIUS 代理服务器接收访问请求消息，并基于本地配置的连接请求策略确定将访问请求消息转发到哪里。
- ✧ IAS RADIUS 代理服务器将访问请求消息转发到相应的 RADIUS 服务器。
- ✧ RADIUS 服务器对访问请求消息进行评估。
- ✧ 如果需要，RADIUS 服务器将向 IAS RADIUS 代理服务器发送访问质询消息，在此处，此消息将被转发到访问服务器；访问服务器通过访问客户端处理质询，并向 IAS RADIUS 代理服务器发送更新的访问请求，在此处，该请求将被转发到 RADIUS 服务器。
- ✧ RADIUS 服务器对连接尝试进行身份验证和授权。
- ✧ 如果已对连接尝试进行身份验证和授权，RADIUS 服务器将向 IAS RADIUS 代理服务器发送访问-接受消息，在此处，该消息将被转发到访问服务器；如果未对连接尝试进行身份验证或授权，RADIUS 服务器将向 IAS RADIUS 代理服务器发送访问-拒绝消息，在此处，该消息将被转发到访问服务器。
- ✧ 访问服务器完成与访问客户端的连接进程，并向 IAS RADIUS 代理发送记账统计请求消息。IAS RADIUS 代理服务器记录记账统计数据，并向 RADIUS 服务器转发此消息。
- ✧ RADIUS 服务器向 IAS RADIUS 代理服务器发送记账统计响应消息，在此处，此响应将被转发到访问服务器。

2. 安装 IAS

IAS 是 Windows Server 2003 组件之一，其安装过程很简单，具体如下所述。

❶ 依次单击【开始】→【控制面板】→【添加或删除程序】菜单，在打开的【添加或删除程序】窗口中，单击【添加/删除 Windows 组件】图标，如图 6-72 所示。

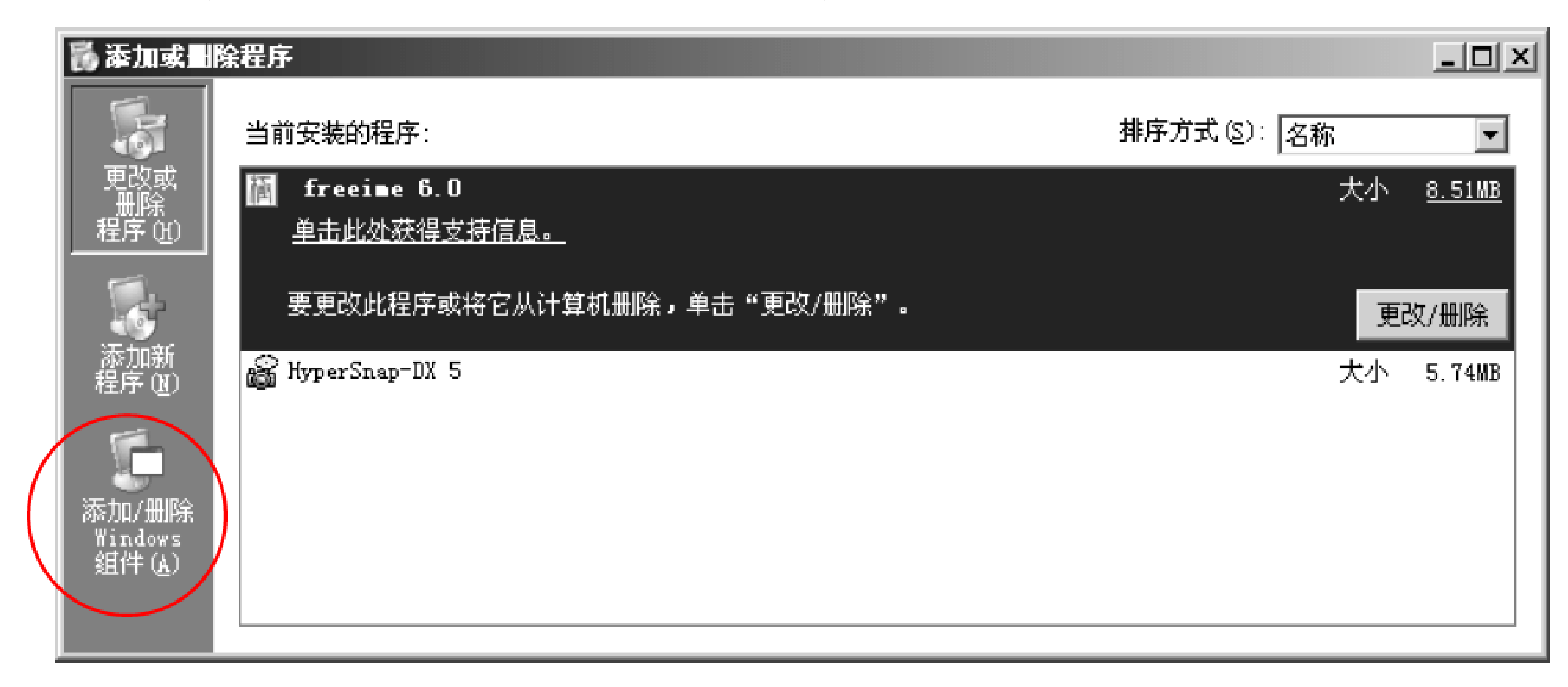


图 6-72 【添加或删除程序】窗口

❷ 在【Windows 组件向导】对话框中，在【组件】列表框中选择【网络服务】选项，然后单击【详细信息】按钮，在弹出的【网络服务】对话框中选择【Internet 验证服务】选项，如图 6-73 所示。

❸ 选择后单击【确定】按钮，然后在 Windows 组件向导中单击【下一步】按钮，直到完成 IAS 的安装。



图 6-73　Windows 组件向导

❹ 依次单击【开始】→【程序】→【管理工具】→【Internet 验证服务】菜单，打开【Internet 验证服务】控制台窗口，通过该控制台窗口就可以进行 IAS 的配置了，如图 6-74 所示。

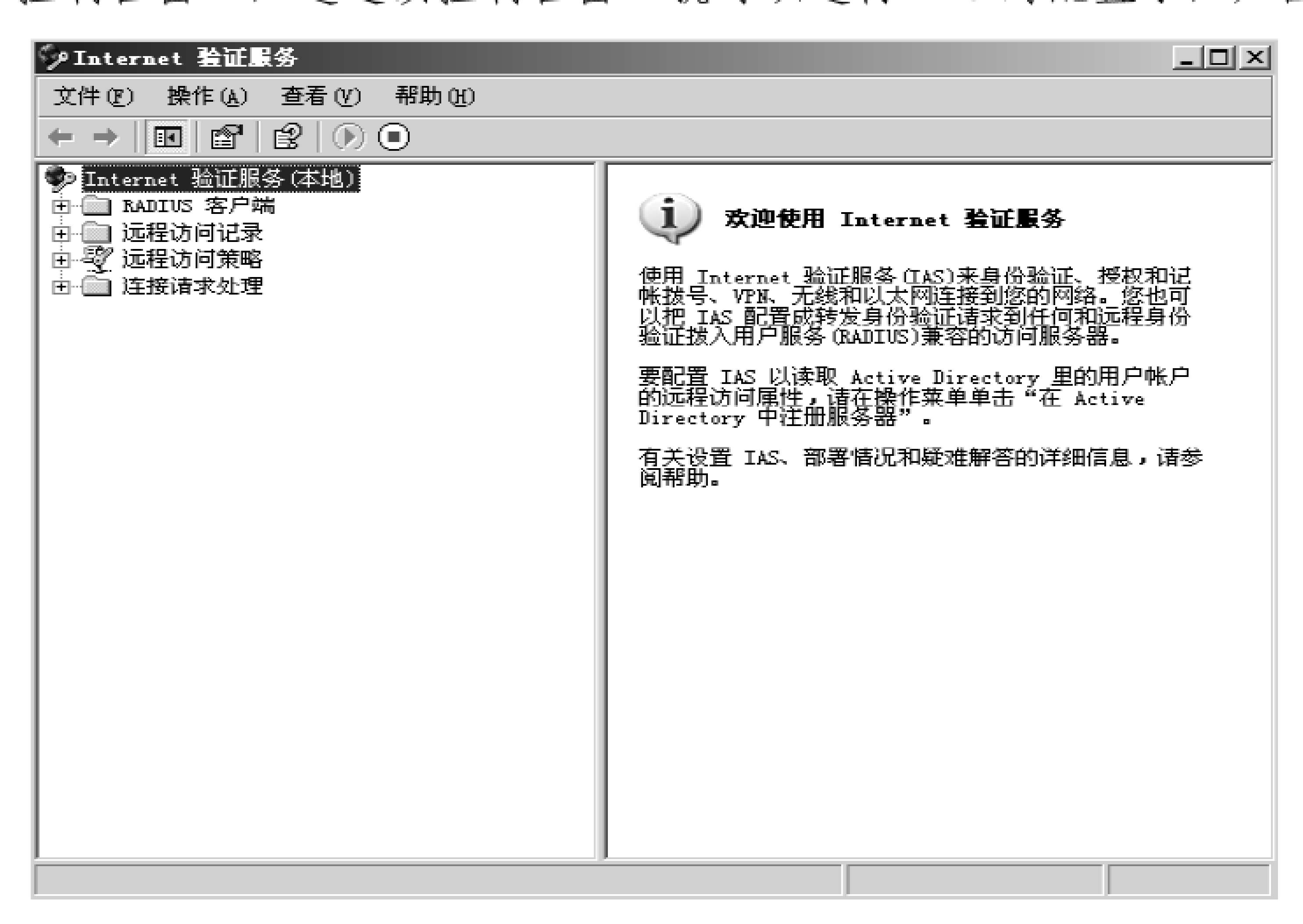


图 6-74　配置 IAS

3. 注册 IAS

当 IAS 注册到 Active Directory 后，它将读取 Active Directory 中的用户账户。当用户以 AD 用户账户身份连接时，IAS 服务器将向域控制器查询用户账号信息，确定用户是否有连接权限。注册 IAS 可按如下步骤进行。

❶ 打开【Internet 验证服务】控制台窗口，右键单击【Internet 验证服务】图标，在弹出的快捷菜单中选择【在 Active Directory 中注册服务器】命令，如图 6-75 所示。



图 6-75 【Internet 验证服务】控制台窗口

❷ 在打开的【在 Active Directory 中注册 "Internet 验证服务器"】对话框中，单击【确定】按钮，如图 6-76 所示。

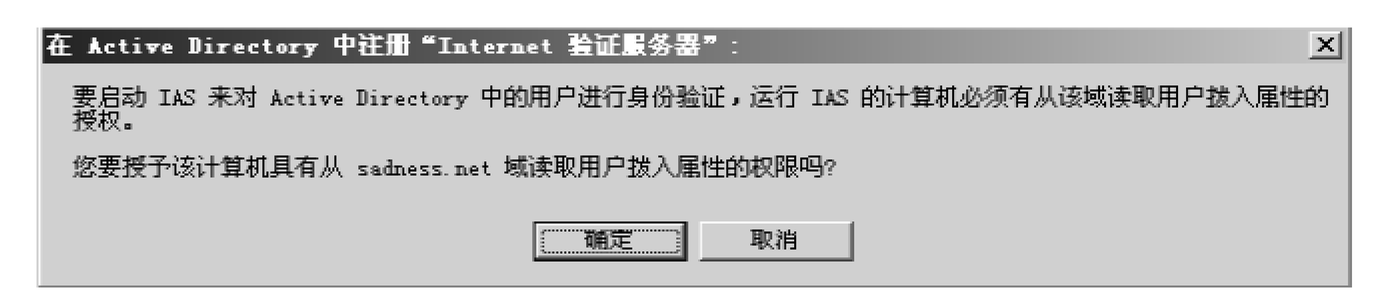


图 6-76 【在 Active Directory 中"注册 Internet 验证服务器"】对话框

❸ 也可以直接运行命令行来注册 IAS 服务器，如图 6-77 所示。



图 6-77 以命令行注册 Internet 验证服务

4. 添加/删除 RADIUS 客户端

IAS 服务器无论在 RADIUS 服务器模式，或者 RADIUS 代理服务器模式，都必须指定

其 RADIUS 客户端，因为它们只接受这些指定的 RADIUS 客户端传来的连接请求，并提供相应的服务。添加 RADIUS 客户端的方式如下。

❶ 打开【Internet 验证服务】控制台窗口，右键单击【RADIUS 客户端】图标，在弹出的快捷菜单中选择【新建 RADIUS 客户端】命令，将弹出【新建 RADIUS 客户端】对话框，如图 6-78 所示。



图 6-78　添加 RADIUS 客户端

❷ 在【名称和地址】向导页中，为 RADIUS 客户端输入名称及其 IP 地址，并单击【下一步】按钮，如图 6-79 所示。



图 6-79　【新建 RADIUS 客户端】对话框

❸ 在【其他信息】向导页中，选择客户端-供应商和共享机密。如果是 Windows Server 系列服务器，则选择 Microsoft；如果是 Cisco 生产的 NAS，则选择 Cisco；当不知道设备是哪个供应商时，选择 RADIUS Standard。【共享的机密】是设置 RADIUS 客户端访问 IAS 的密码选项，当使用 PAP、CHAP、MS-CHAP 以及 MS-CHAP v2 进行身份验证时，启用消息验证程序属性可以提供附加的安全性。默认情况下，EAP 使用消息验证程序属性，因而不要求启用该属性。设置完毕后单击【下一步】按钮，如图 6-80 所示。

❹ 重复上述步骤，可以指定多台 RADIUS 客户端。

❺ 在需要作为 RADIUS 客户端的设备上配置 RADIUS。以 Cisco 路由器为例，可以使用 radius-server host 命令来配置，其中的“key”就是我们设置的“共享机密”密码。

```
Router(config)#radius-server host 10.0.0.2 auth_port 1645 acct-port 1646 key
Cisco
```

❻ 如果需要删除一个 RADIUS 客户端，则在详细信息窗格中，右键单击要删除的客户端，然

后在弹出的快捷菜单中选择【删除】命令，如图 6-81 所示。

图 6-80　设置客户端及共享机密

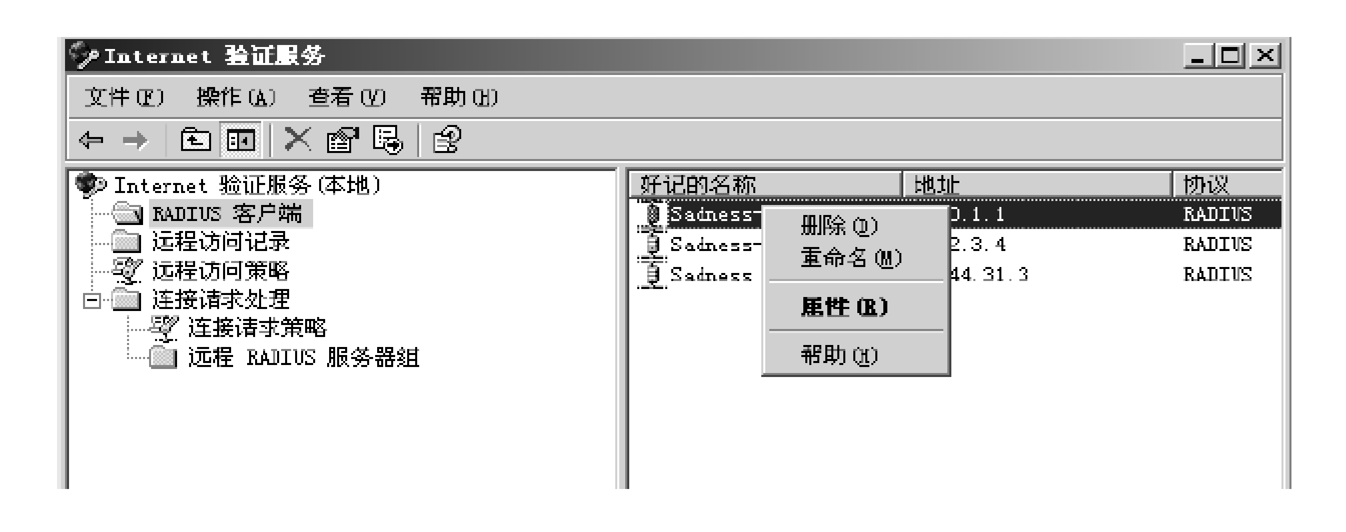


图 6-81　删除 RADIUS 客户端

5. 配置 RADIUS 代理服务器

通常仅有一台 RADIUS 服务器是相对不安全的，当这台服务器受到攻击下线后，所有用户将无法使用身份认证。如果受到攻击时有多台 RADIUS 服务器，则可以使用负载均衡，降低被攻陷的可能性。在这种情况下，通常将一台 IAS 服务器设置成 RADIUS 代理服务器，同时把另外几台 IAS 服务器设置为 RADIUS 服务器。配置 RADIUS 代理服务器由 IAS 的"连接请求策略"功能来设置。连接请求策略是条件和配置文件设置的集合，网络管理员可以使用连接请求策略，灵活地配置 IAS 服务器处理传入的身份验证和记账统计请求消息的方式。使用连接请求策略，可以创建一系列的策略，从而可以在本地处理从 RADIUS 客户端发送的某些 RADIUS 请求消息(IAS 用作 RADIUS 服务器)，并可以将其他类型的消息转发至另一台 RADIUS 服务器(IAS 用作 RADIUS 代理)。使用此功能可以在多种新 RADIUS 方案中配置 IAS 服务器。

配置 RADIUS 代理服务器的方法如下。

❶ 打开【Internet 验证服务】控制台窗口，在【连接请求处理】下右键单击【远程 RADIUS 服务器组】图标，在弹出的快捷菜单中选择【新建远程 RADIUS 服务器组】命令，如图 6-82 所示。

❷ 在新建远程 RADIUS 服务器组向导中直接单击【下一步】按钮。在【新配置方法】向导页中，选择服务器组的类型和组名，单击【下一步】按钮，如图 6-83 所示。



图 6-82　新建远程 RADIUS 服务器组

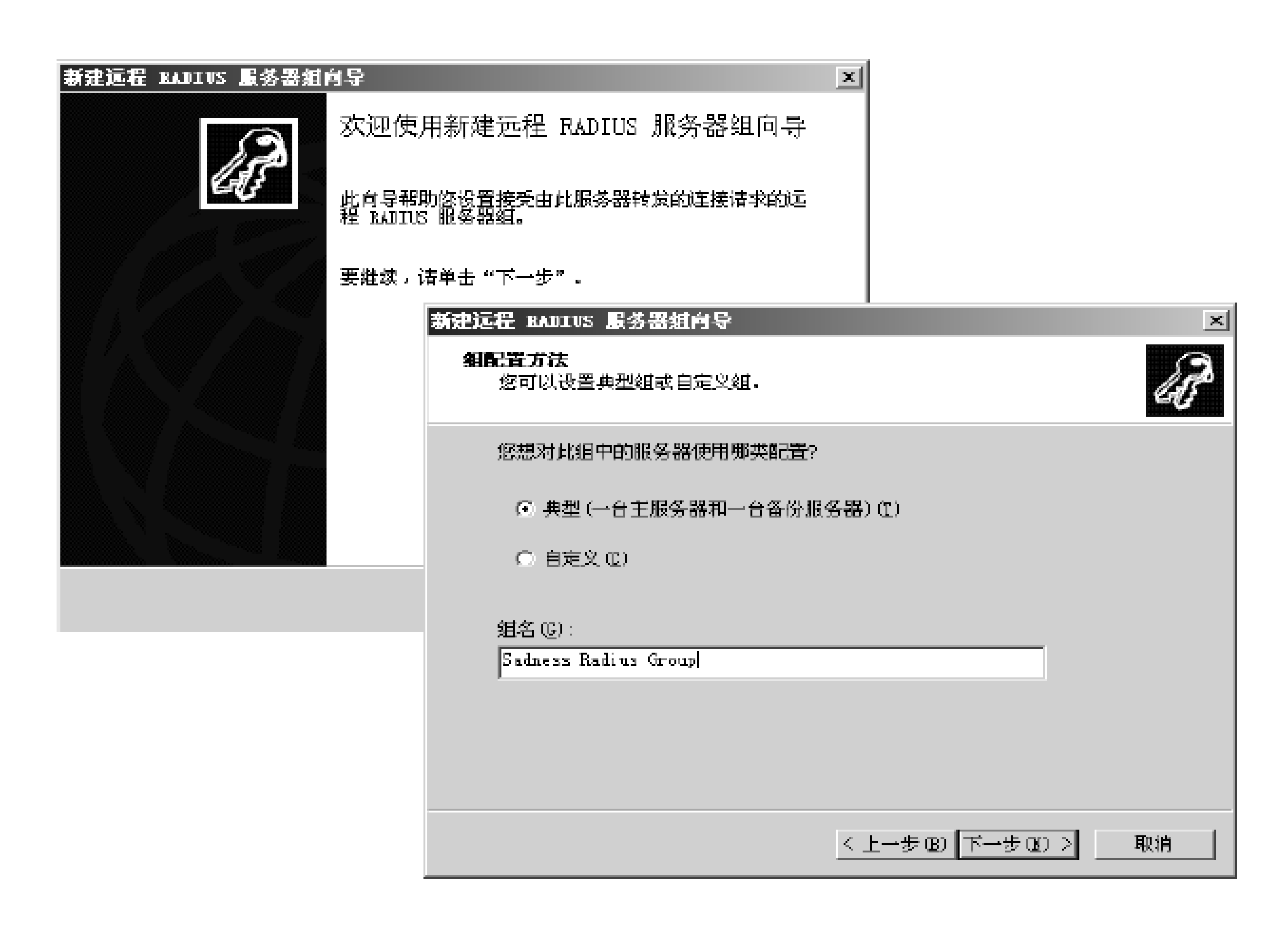


图 6-83　选择服务器的类型和组名

❸ 在【添加服务器】向导页中，设置主服务器和备份服务器的 IP 地址，以及服务器组的共享密码。设置完毕后，单击【下一步】按钮，如图 6-84 所示。

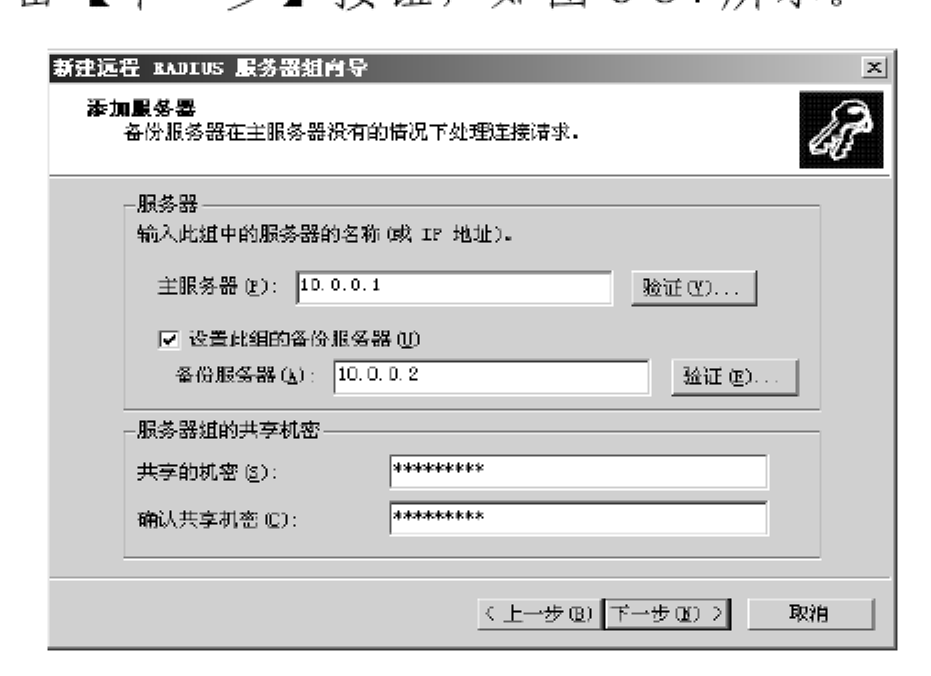


图 6-84　设置主服务器和备份服务器

❹ 完成新建远程 RADIUS 服务器组向导后，显示确认设置信息，单击【完成】按钮，如图 6-85 所示。

❺ 若在第❹步中选中【当此向导关闭时启动“新建连接请求策略向导”】复选框，将打开新建连接请求策略向导，直接单击【下一步】按钮。在【策略配置方法】向导页中，定义策略并输入策略名。设置完毕后，单击【下一步】按钮，如图 6-86 所示。

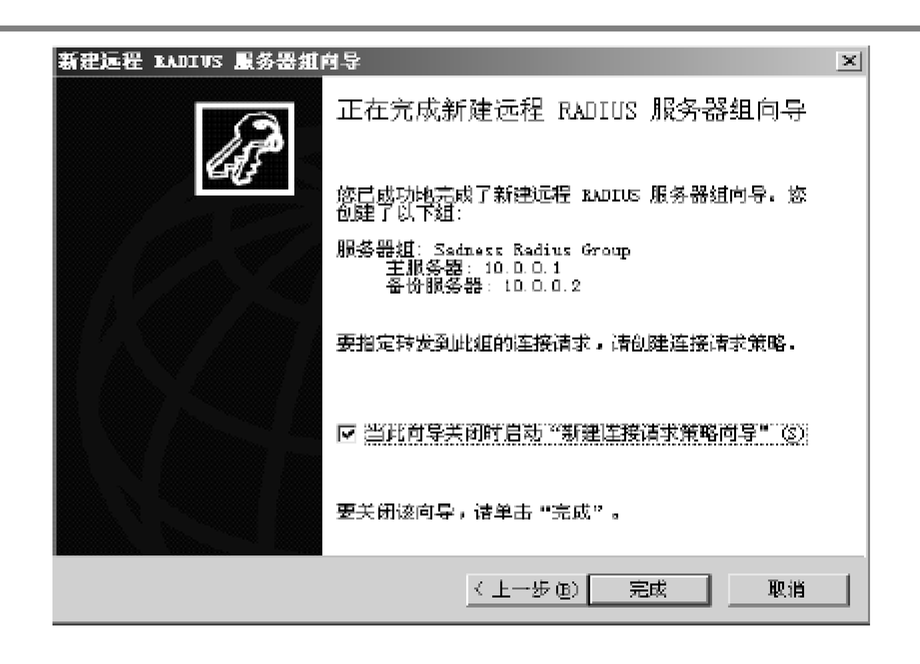


图 6-85　完成配置



图 6-86　新建连接请求策略向导

❻ 在【请求身份验证】向导页中，选中【转发连接请求到远程 RADIUS 服务器作身份验证】单选按钮，并单击【下一步】按钮。在【领域名】向导页中，输入领域名并选定前面定义的 RADIUS 服务器组，单击【下一步】按钮，如图 6-87 所示。



图 6-87　选定服务器组

7. 完成新建连接请求策略向导后，显示确认设置信息，单击【完成】按钮。
8. 如果需要定义新的连接策略，我们可以在【Internet 验证服务】控制台窗口中，依次选择【连接请求处理】→【连接请求策略】→【对所有用户使用】选项，右击，在弹出的快捷菜单中选择 【属性】命令，如图 6-88 所示。

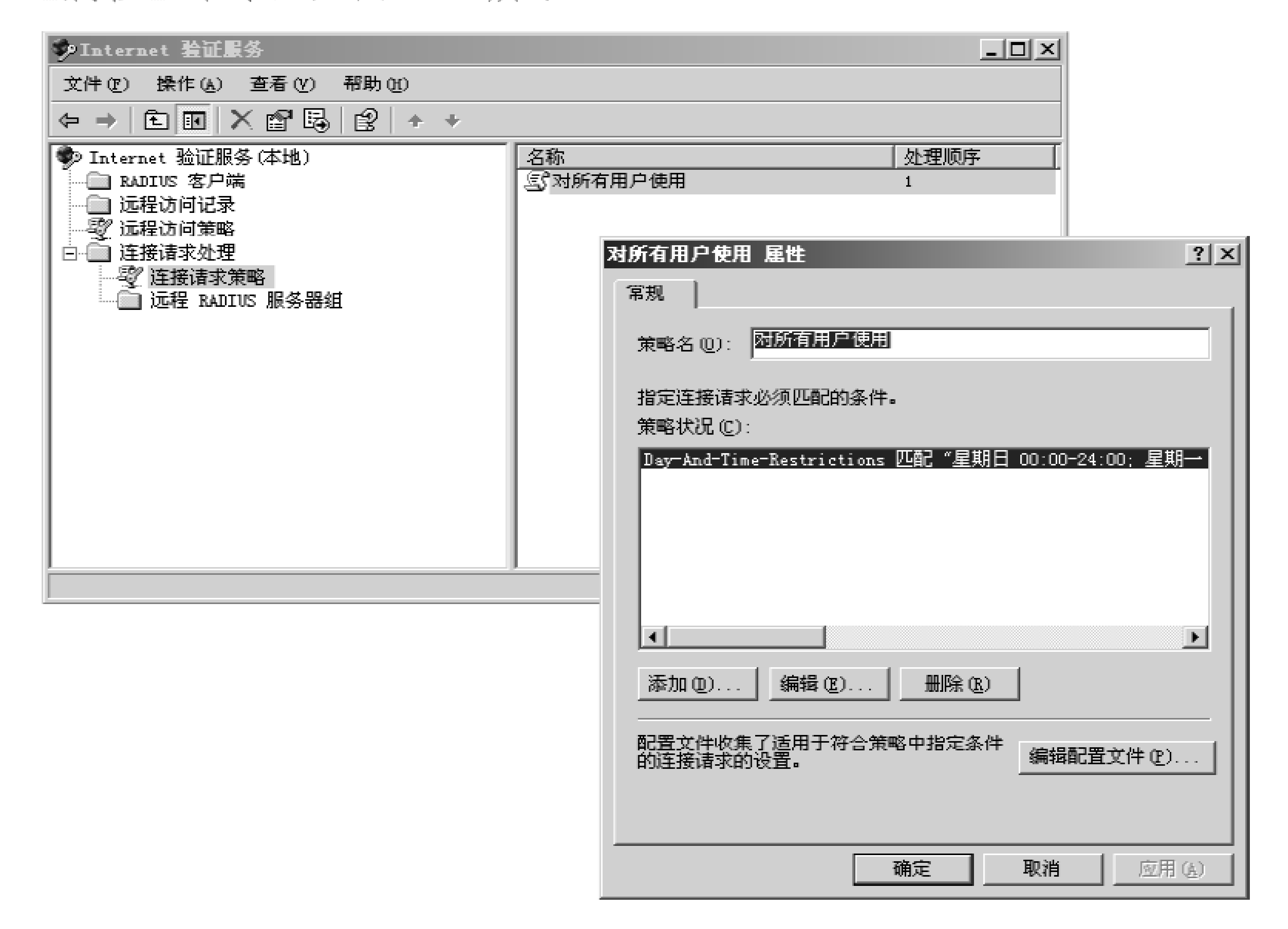


图 6-88　连接请求策略

9. 在图 6-88 中，可以看到匹配的是“星期一到星期日的 00:00-24:00”。然后单击【编辑配置文件】按钮，在打开【编辑配置文件】的对话框中选中【把请求转发到下面的远程 RADIUS 服务器组作身份验证】单选按钮，如图 6-89 所示。

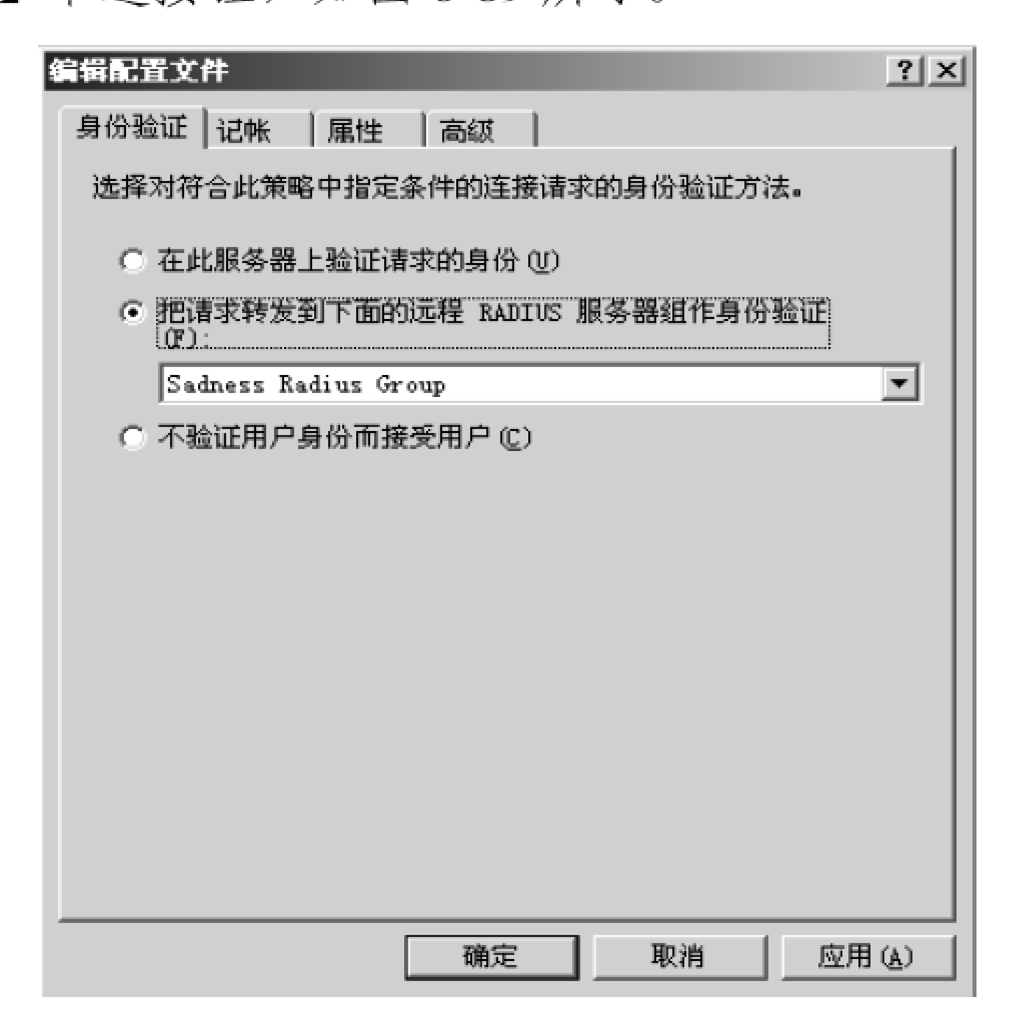


图 6-89　【编辑配置文件】对话框

10. 如果网络中有多台 RADIUS 服务器，还可以设置远程 RADIUS 服务器组。设置方法是，在

【Internet 验证服务】控制台窗口中，选择【连接请求处理】→【远程 RADIUS 服务器组】选项，再用鼠标右键单击配置的 Sadness Radius Group 选项，在弹出的快捷菜单中选择【属性】命令；在弹出的对话框中，单击【添加】按钮为服务器组添加新的 RADIUS 服务器，如图 6-90 所示。



图 6-90 添加新的 RADIUS 服务器

11 用户还可以添加新 RADIUS 服务器的优先级。设置方法是，用鼠标右键单击其中一台服务器，在弹出的快捷菜单中选择【属性】命令，切换到【负载平衡】选项卡，设置不同的负载分担方式，如图 6-91 所示。

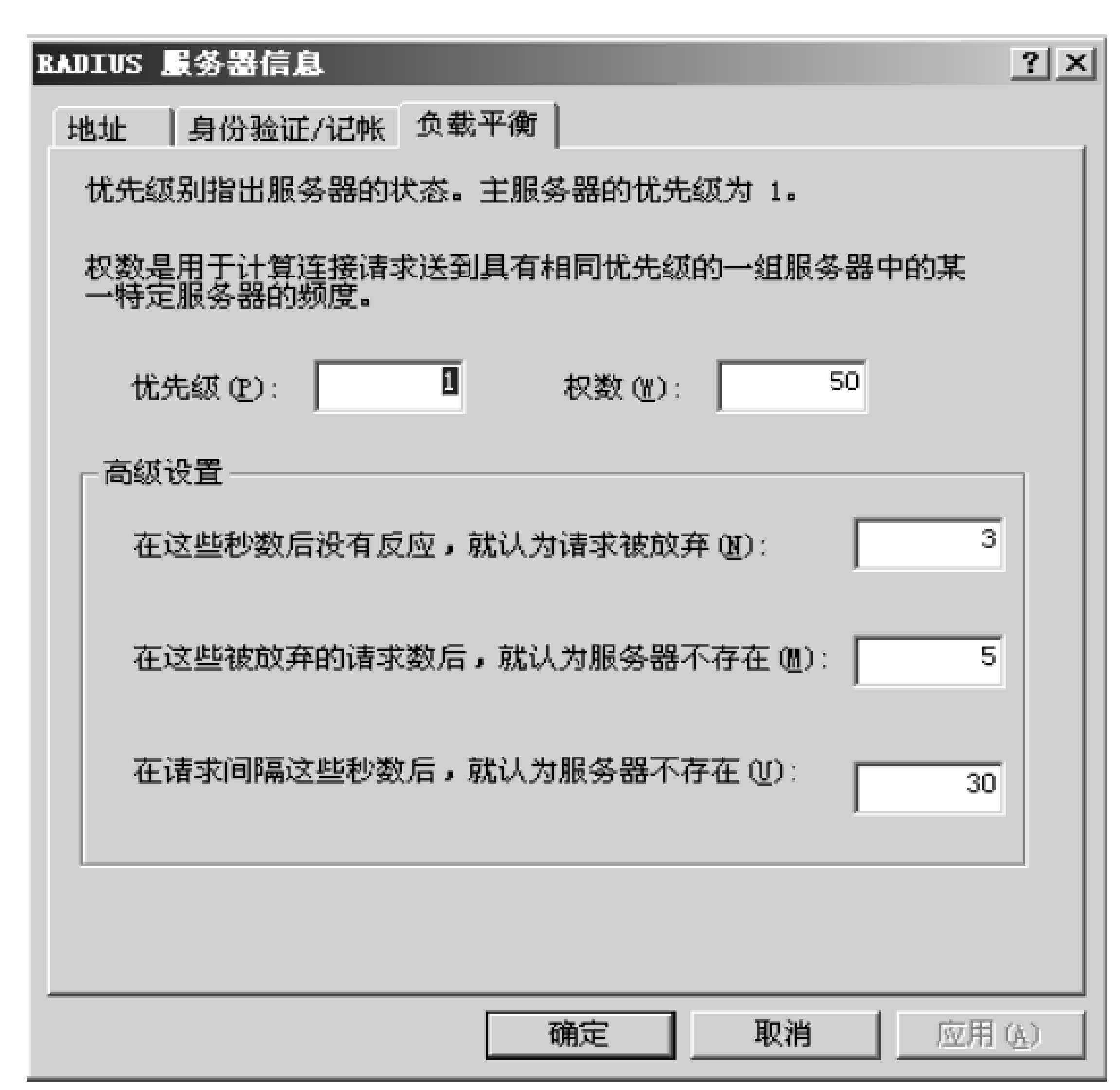


图 6-91 配置 RADIUS 服务器组负载平衡

至此，我们完成了基于微软IAS的RADIUS服务器配置，下面一节将介绍Cisco的Secure ACS服务器配置方案。

6.3.3　Cisco Secure ACS

1. Cisco Secure ACS 简介

Cisco Secure ACS (ACS，Access Control Server)是具高可扩展性的高性能访问控制服务器，可作为集中的RADIUS 和 TACACS+ 服务器运行。Cisco Secure ACS将验证、用户访问和管理员访问与策略控制结合在一个集中的身份识别网络解决方案中，因此提高了灵活性、移动性、安全性和用户生产率，从而进一步增强了访问安全性。它针对所有用户执行统一安全策略，不受用户网络访问方式的影响，减轻了与扩展用户和网络管理员访问权限相关的管理负担。通过对所有用户账户使用一个集中数据库，Cisco Secure ACS可集中控制所有的用户权限并将它们分配到网络中的几百甚至几千个接入点。对于记账统计服务，Cisco Secure ACS针对网络用户的行为提供具体的报告和监控功能，并记录整个网络上每次的访问连接和设备配置变化。这个特性对于企业遵守Sarbanes Oxley法规尤其重要。Cisco Secure ACS支持广泛的访问连接，包括有线/无线局域网、宽带、内容、存储、IP上的语音(VoIP)、防火墙和VPN等。

Cisco Secure ACS是思科基于身份验证的网络服务(IBNS)架构的重要组件。Cisco IBNS基于802.1x (用于基于端口的网络访问控制的IEEE标准)和可扩展验证协议(EAP)等端口安全标准，并将安全验证、授权和记账统计(AAA)从网络外围扩展到了LAN中的每个连接点。您可在这个全新架构中部署新的策略控制工具(如每个用户的配额、VLAN分配和访问控制列表(ACL))，这是因为思科交换机和无线接入点的扩展功能可用于在RADIUS协议上查询Cisco Secure ACS。

Cisco Secure ACS也是思科网络准入控制(NAC)架构的重要组件。思科NAC是思科系统公司赞助的业界计划，使用网络基础设施迫使试图访问网络计算资源的所有设备遵守安全策略，进而防止病毒和蠕虫造成损失。通过NAC，客户只允许遵守安全策略的可信的端点设备访问网络(如PC、服务器和个人数字助理等)，并可限制违规设备的访问。思科NAC是思科自防御网络计划的一部分，为在第二层和第三层网络上实现网络准入控制奠定了基础。我们计划进一步扩展端点和网络安全性的互操作性，以便将动态的事故抑制功能包含在内。这个创新将允许遵守安全策略的系统组件报告攻击期间因恶意系统或受感染的系统导致的资源误用。因此，用户可将受感染的系统与其他网络部分动态隔离开，从而大大减少病毒、蠕虫及混合攻击的传播。

2. 安装 Cisco Secure ACS

与一般软件一样，Cisco Secure ACS的安装过程非常简单，只需根据安装向导做简单配置即可，下面简要地介绍其安装过程。

❶ 在Cisco网站上下载Cisco Secure ACS for Windows，双击Setup.exe开始安装，如图6-92所示。

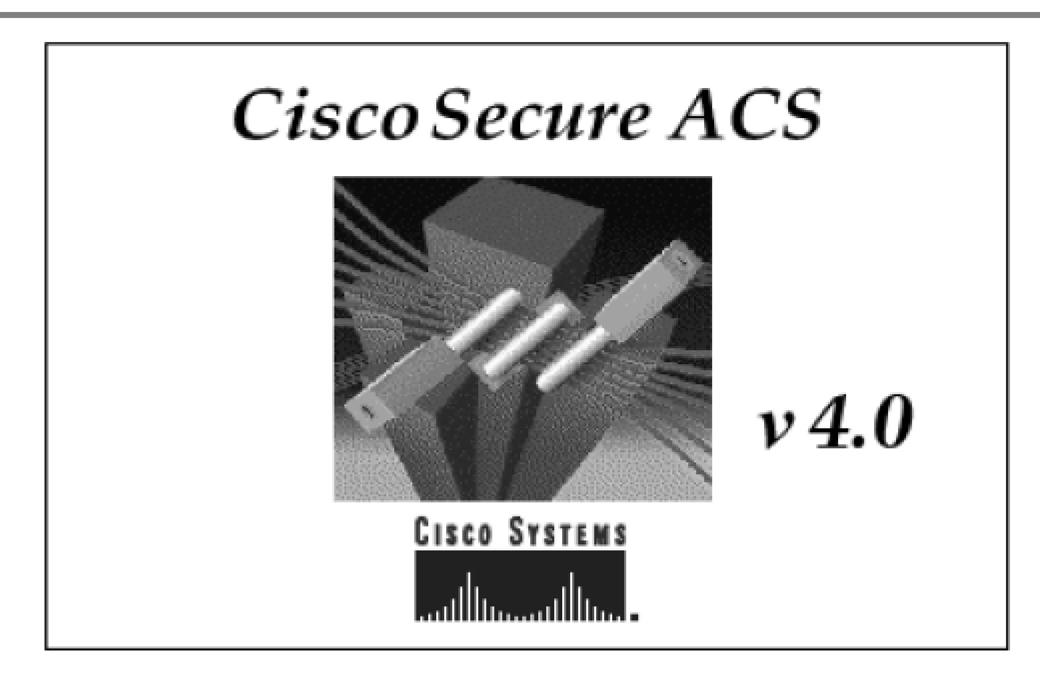


图 6-92　安装 Cisco Secure ACS 4.0

❷ 在是否同意 Cisco Secure ACS 的软件协议窗口中，单击 ACCEPT 按钮继续安装，如图 6-93 所示。

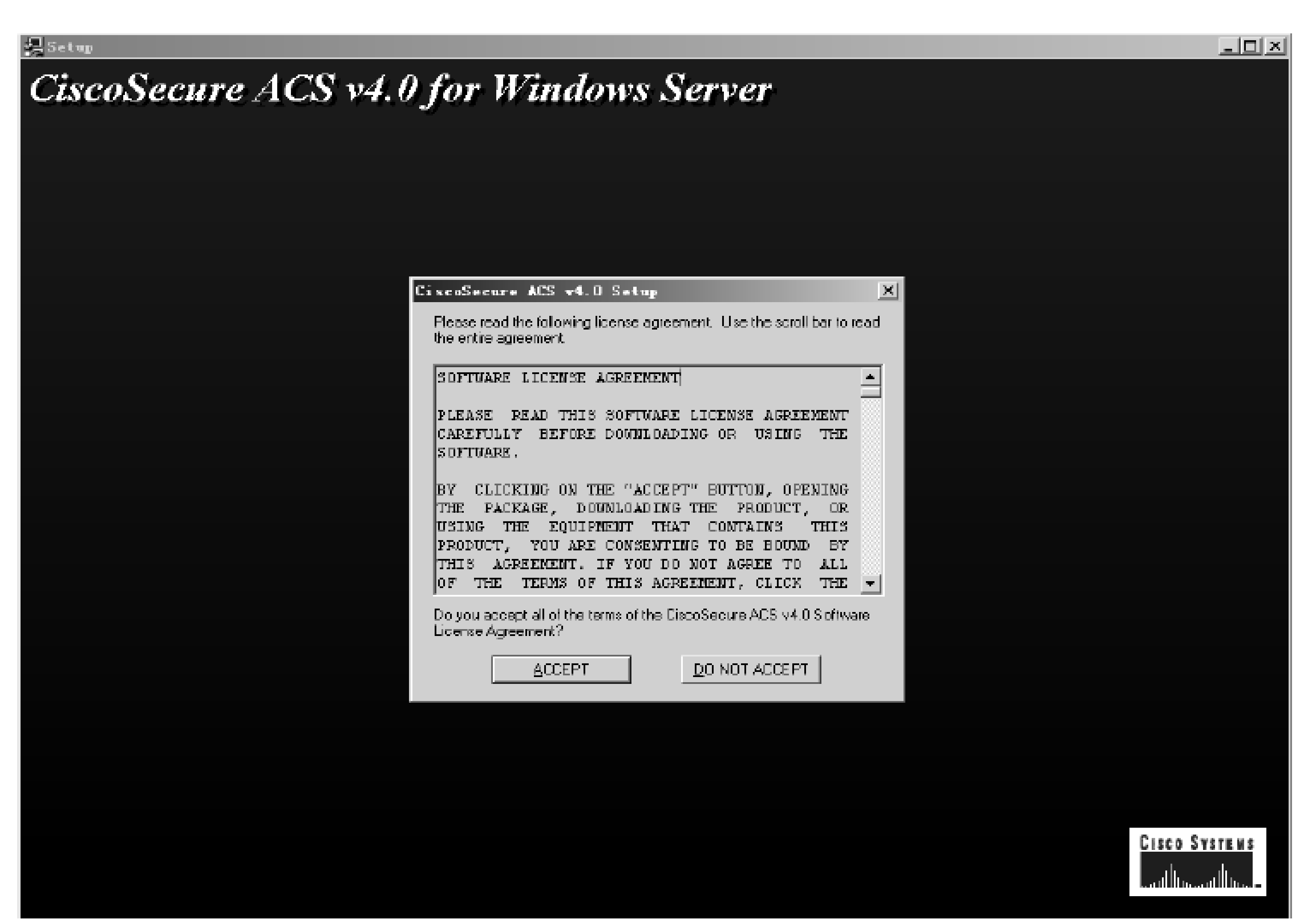


图 6-93　安装 Cisco Secure ACS 4.0

❸ 在出现欢迎界面后，直接单击 Next 按钮。如果系统已经安装了微软 IAS 服务器，则安装时会提示是否禁用 IAS。这是由于 RADIUS 使用相同的默认端口，同时运行两个 RADIUS 服务器进程会出现一些问题，我们建议用户如果选择 Cisco Secure ACS 服务器，则选择禁用 IAS，如图 6-94 所示。

❹ 选择禁用 IAS 后，系统会要求自动重启，单击【确定】按钮并重新启动服务器。然后再次运行 Setup.exe 进行 Cisco Secure ACS 安装。在安装前选择终端用户能够成功连接到 AAA 客户端，并选择 Windows 服务器是否能够 ping 通 AAA 客户端，同时还可以选择任何使用 Cisco IOS 系统的 AAA 客户端能够被支持等，然后单击 Next 按钮，如图 6-95 所示。

❺ 选择 Cisco Secure ACS 的安装路径，确认后单击 Next 按钮；接着选择 Cisco Secure ACS 是否使用本地独立数据库，或者同时检查 Windows 用户数据库，为了更好的兼容性和管理特性，这里选中 Also check the Windows User Database 单选按钮。单击 Next 按钮，系统开始安装，如图 6-96 所示。

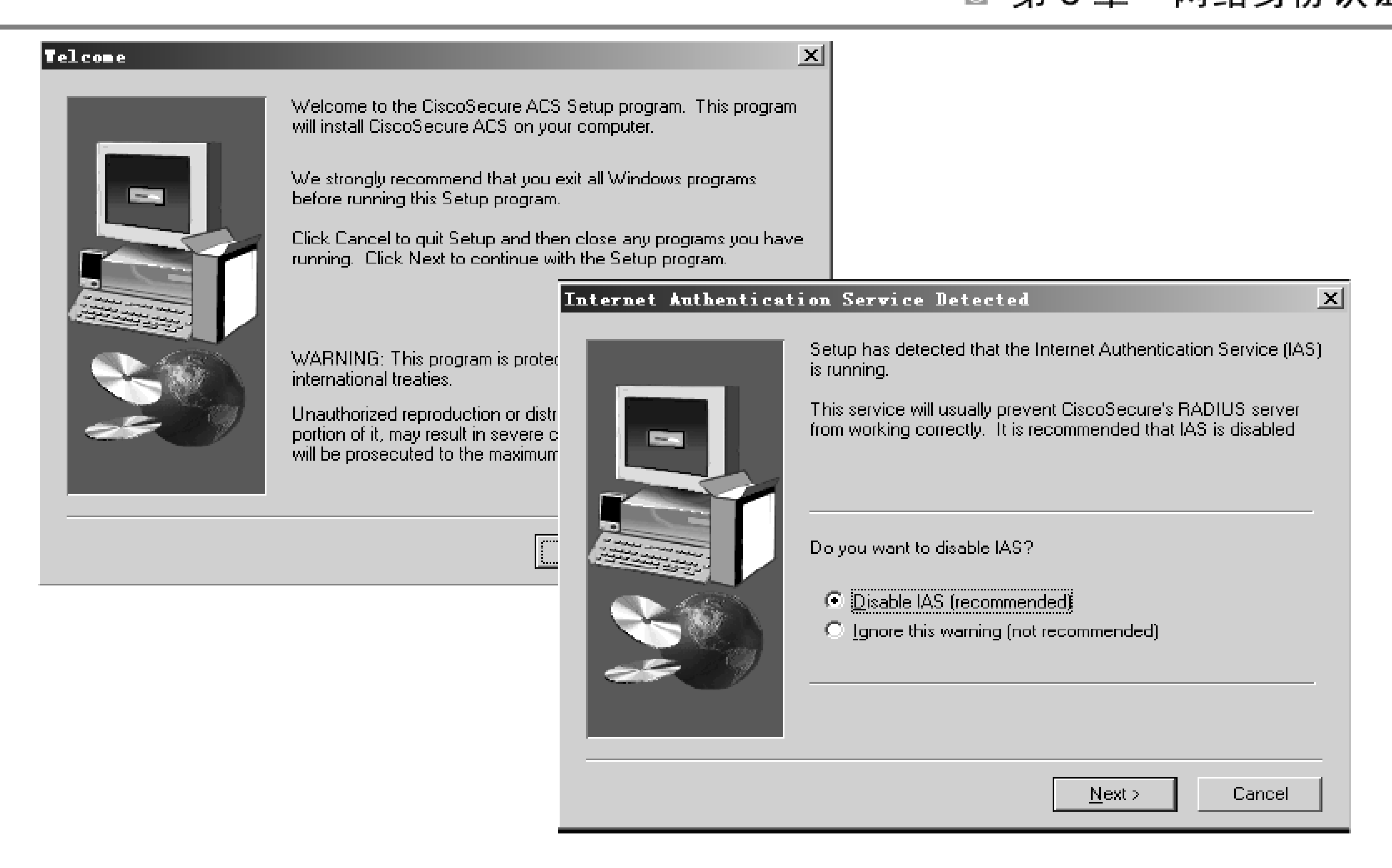


图 6-94　是否禁用 IAS

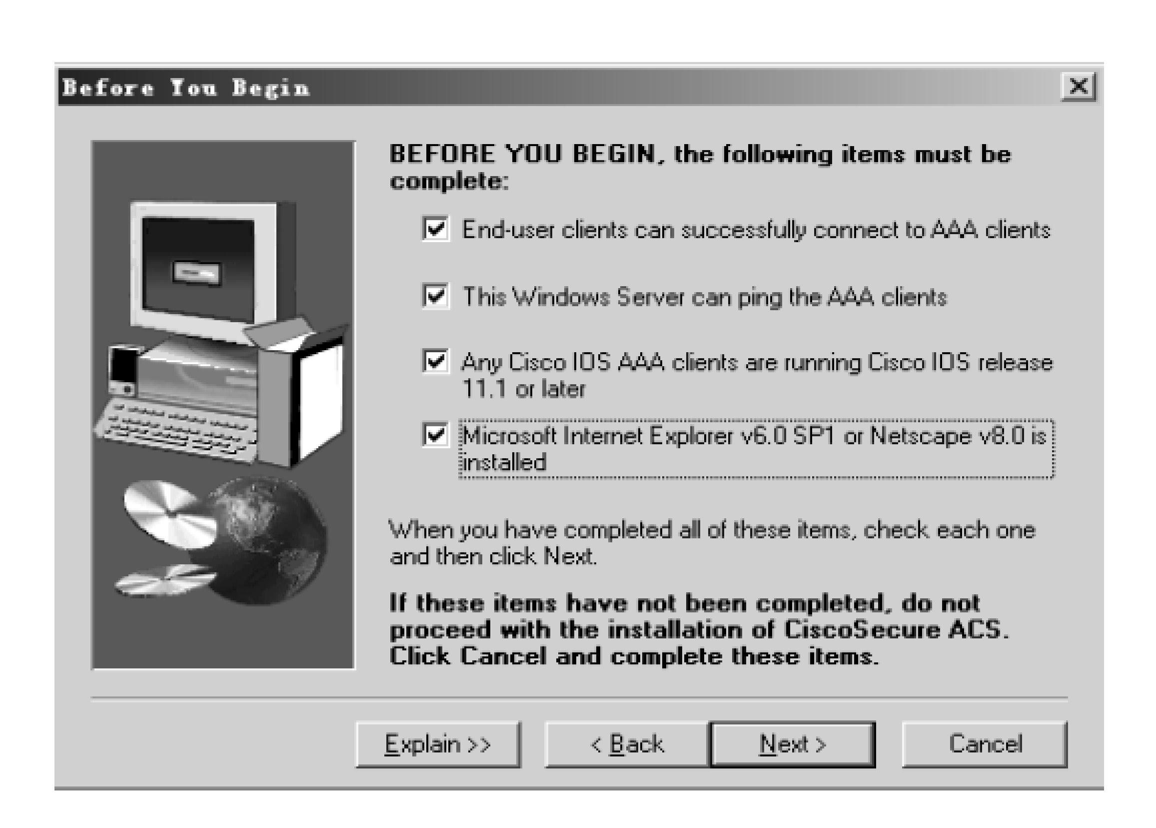


图 6-95　设置选择

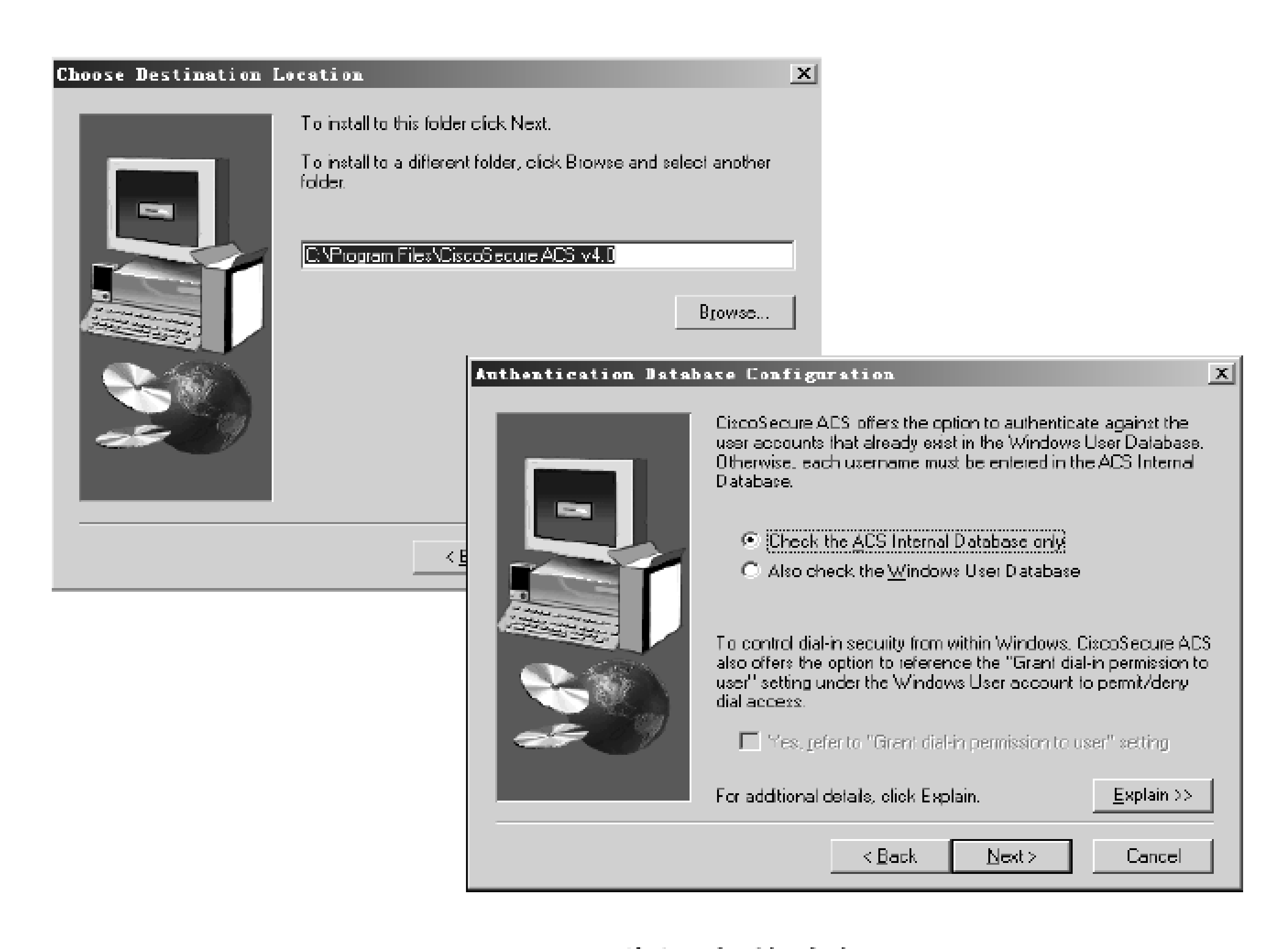


图 6-96　选择安装路径

❻ 完成安装后，将设置高级选项，用户可以根据自己的需求进行设置，确认后单击 Next 按钮。接着，系统会询问是否通过邮件通知等设置，确认后单击 Next 按钮，如图 6-97 所示。

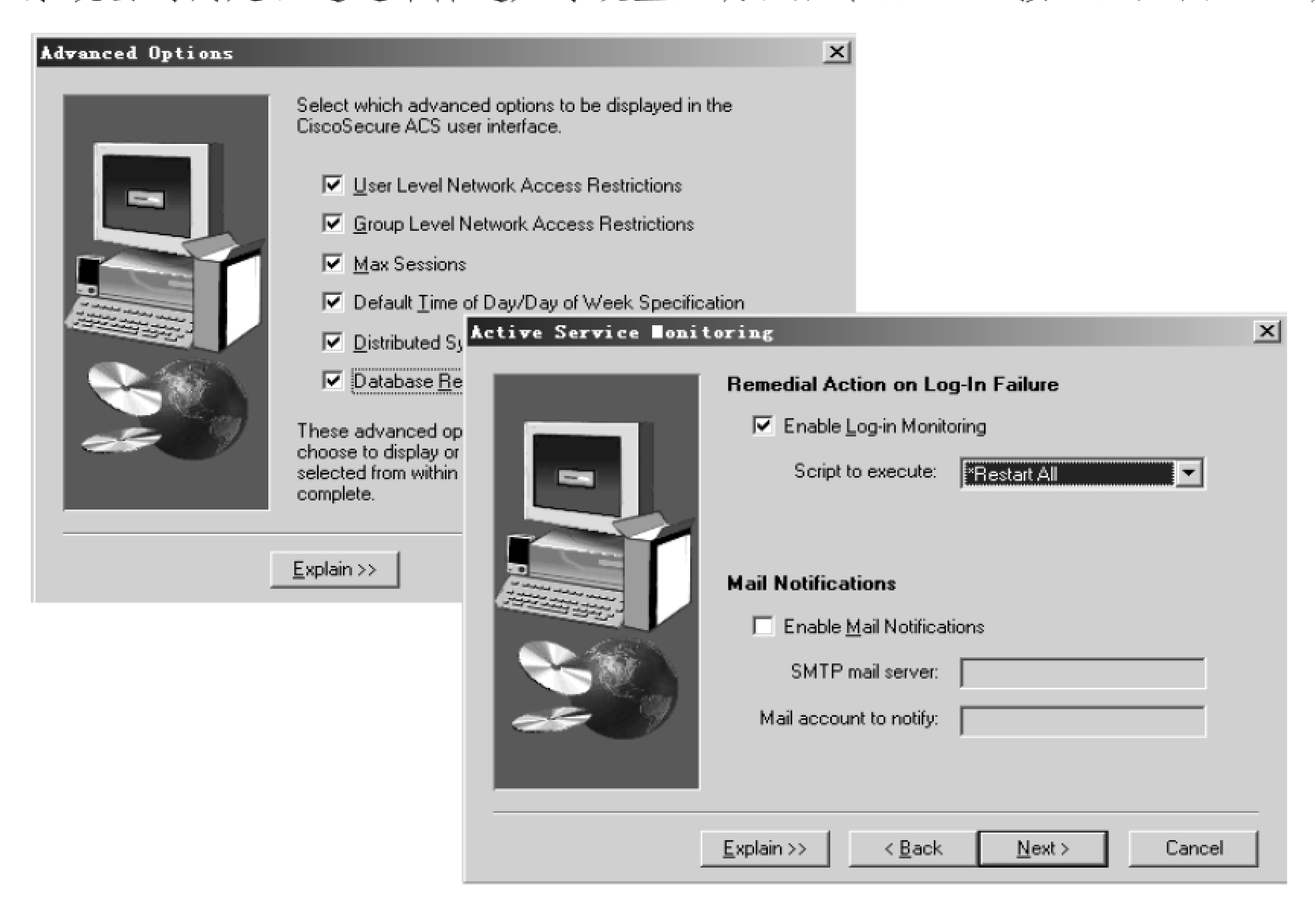


图 6-97　设置高级选项

❼ 系统提示用户输入 ACS 管理账户密码，确认密码无误后，单击 Next 按钮，如图 6-98 所示。

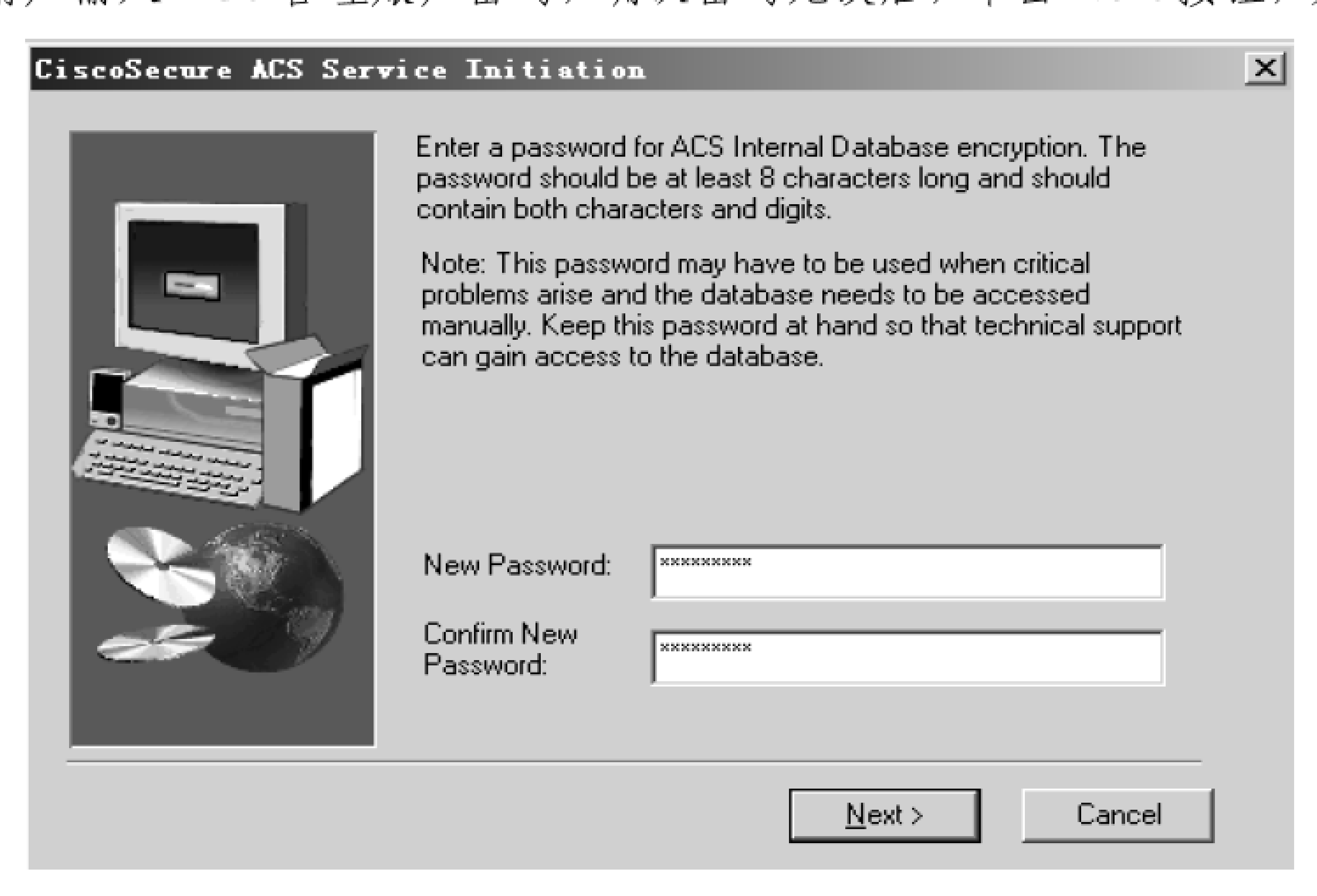


图 6-98　设置密码

❽ 完成安装后使用 ACS，并且询问用户是否在安装完成后阅读用户文档等信息，确认后单击 Finish 按钮。至此，Cisco Secure ACS 安装完毕，并且可以在浏览器地址栏中输入 http://ACS-server-ip:2002，访问 ACS 服务器并对其在本地访问 http://127.0.0.1:2002/对 Cisco Secure ACS 进行配置。

❾ 由于刚安装好的 ACS 服务器没有管理员账号，因此只能在 ACS 服务器上本地访问

http://ACS-server-ip:2002/直接就可以进入 ACS 配置主界面，如图 6-99 所示。

图 6-99　Cisco Secure ACS 4.0 主界面

从图 6-99 中，我们可以看到 Cisco Secure ACS for Windows 主界面分为两部分，其左侧一排按钮为配置导航条，当用户单击导航条中的某个选项时，该选项的具体内容会在右侧显现。ACS 各导航条的功能如下。

- 用户设置(User Setup)：查看、创建、编辑、删除用户账号。
- 组设置(Group Setup)：查看、创建、编辑用户组设置。
- 共享配置组建组件(Shared Profile Components)：一些可共享的授权组件，它们可以应用于一个或多个用户，或用户组。授权组件包括 Network Access Restriction (NAR)、Command authorization set 和 PIX downloadable ACL。
- 网络配置(Network Configuration)：查看、创建、编辑、删除网络服务器(网络设备，如路由器、交换机等)的参数。
- 系统配置(System Configuration)：启动或停止 ACS 服务，创建或删除网络日志，控制 ACS 数据库同步等。
- 接口配置(Interface Configuration)：配置 TACACS+和 RADIUS 的选项。
- 管理控制(Administration Control)：查看、创建、编辑、删除 ACS 的管理员账号参数。
- 外部数据库(External User Database)：配置 ACS 的外部数据库类型以及未知的用户策略。
- 报告和活动(Reports and Activity)：查看 TACACS+和 RADIUS 的审计报告、登录

失败报告以及已经登录的用户信息等。

✧ 在线文档(Online Documentation)：提供关于 Cisco Secure ACS 更详细的文档。

3. 添加 Cisco Secure ACS 管理员账号

Cisco Secure ACS 可以建立多个管理员账号并赋予不同的权限，实现分级权限管理。下面简要地介绍一下建立管理员账号和设置权限的方法。

❶ 添加一个管理员账号到主页中，可以单击 Administration Control 按钮，进入 Administration Control 配置页面。在该页面中，列出了已有的管理员账号列表，并可以新建账号，以及对管理员账号的接入策略(Access Policy)、会话策略(Session Policy)和审计策略(Audit Policy)进行配置，如图 6-100 所示。

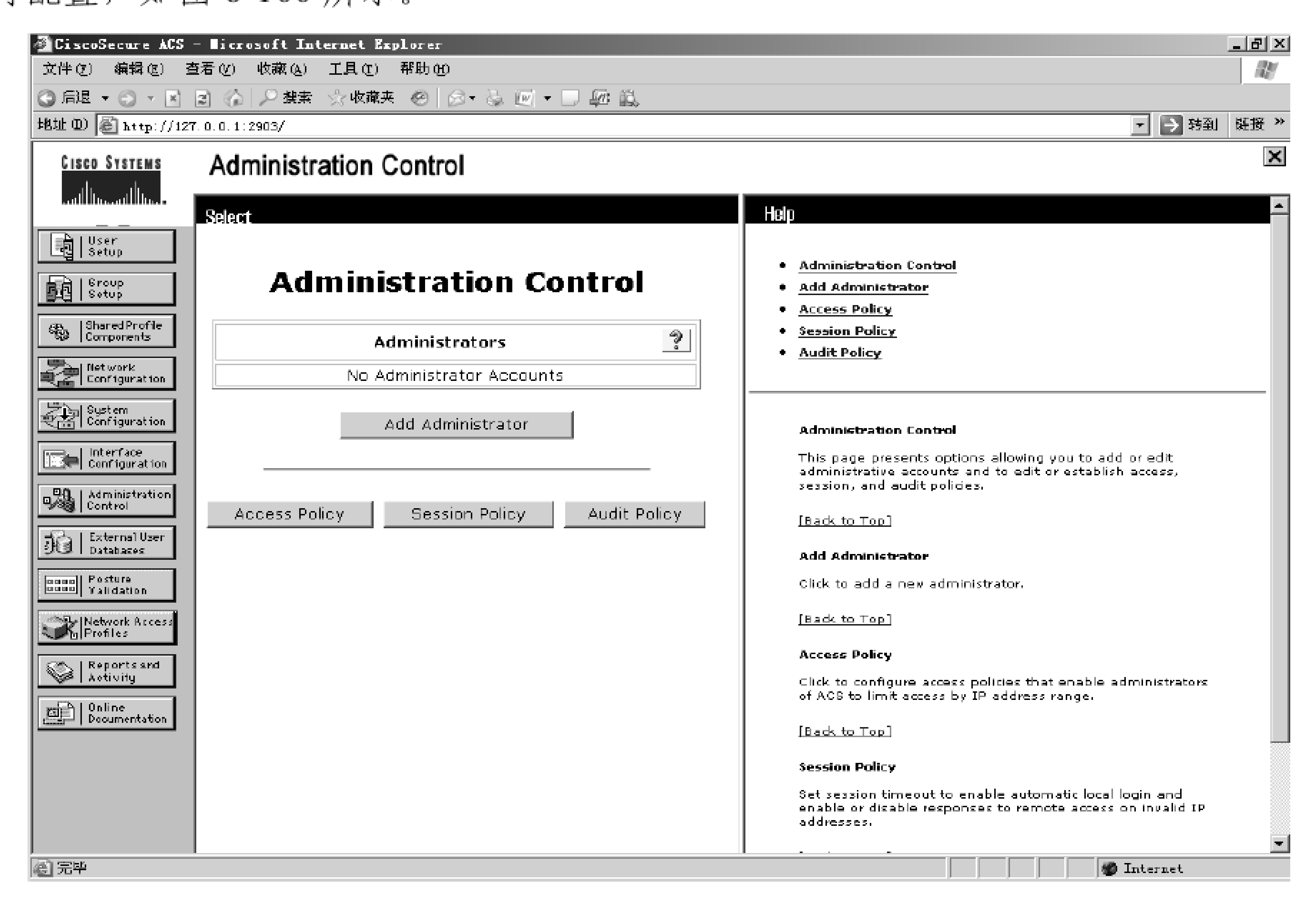


图 6-100　添加管理员账号

❷ 单击 Add Administrator 按钮，即可添加管理员，需要输入用户名和密码，如图 6-101 所示。

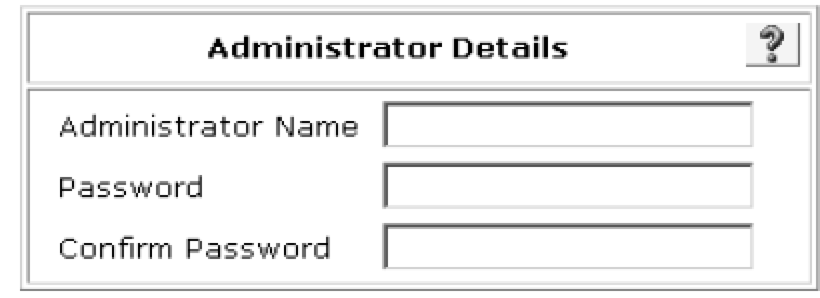


图 6-101　输入管理员账号和密码

❸ 向下滚动配置页，我们可以为该管理员定义各种权限，根据不同的身份选择不同的权限。如果是最高管理员，可以直接选中 Grant All 复选框，赋予全部权限。权限赋予完毕后，单击 Submit 按钮确认，如图 6-102 所示。

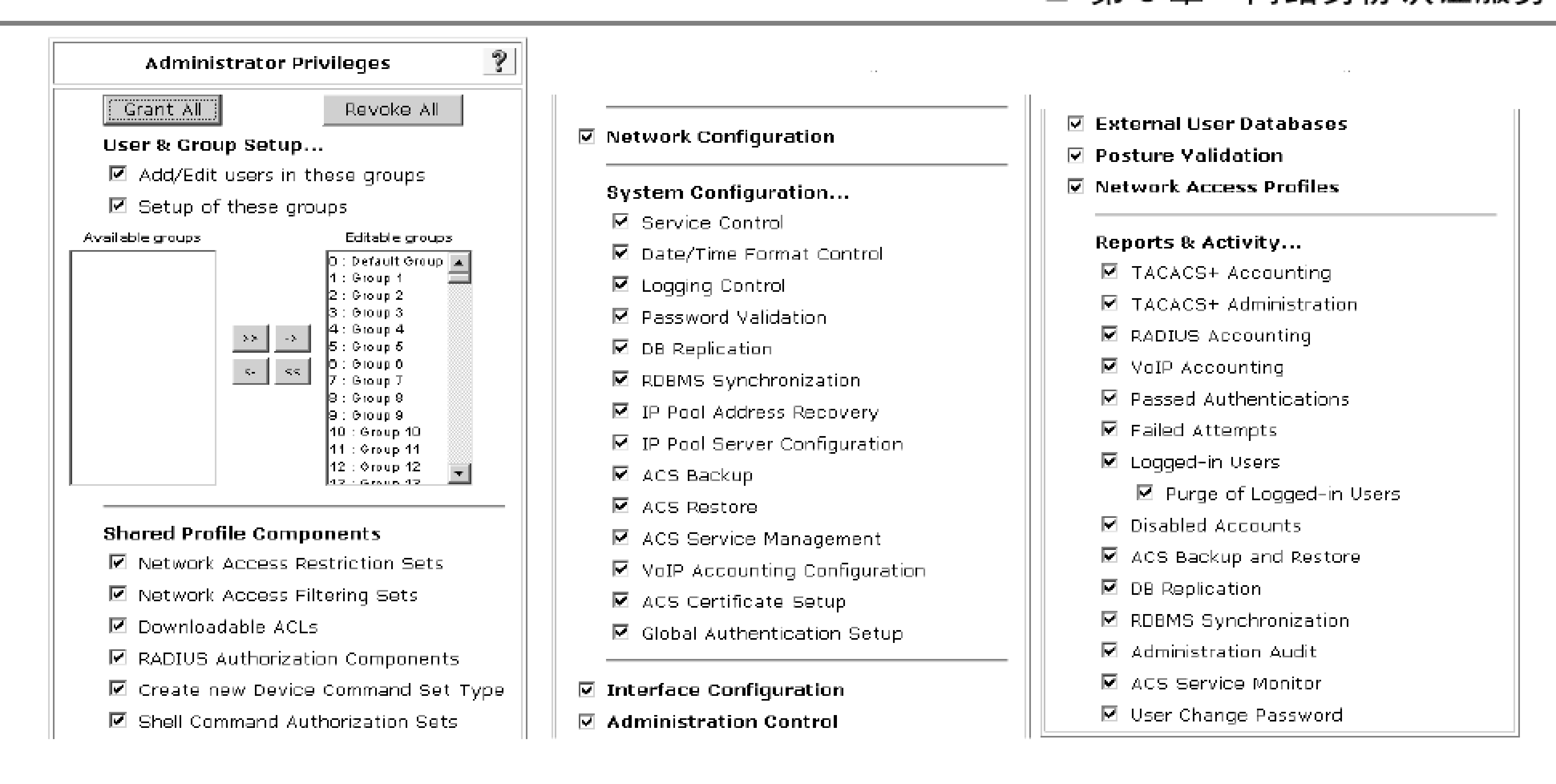


图 6-102　赋予管理账号权限

❹ 返回 Administration Control 界面后，可以对管理员账号的接入策略、会话策略和审计策略进行配置。单击 Access Policy 可以设置接入 IP 地址范围，同时也可以设置 http 接入的选项，选择会话的端口以及是否选择 https 接入，如图 6-103 所示。

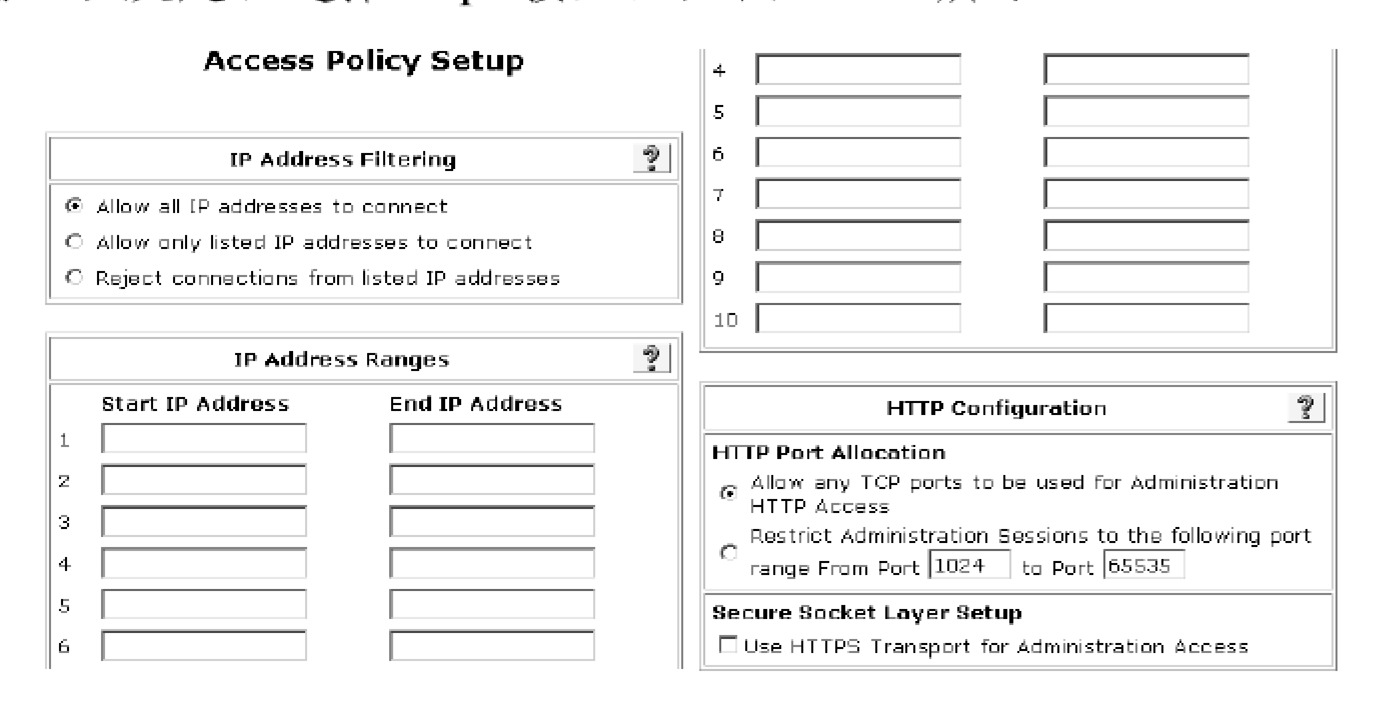


图 6-103　设置 Http 接入的选项

❺ 单击 Session Policy 可以设置会话策略，并选择会话空闲时间，以及多少次失败登录后锁定管理员账号等属性，如图 6-104 所示。

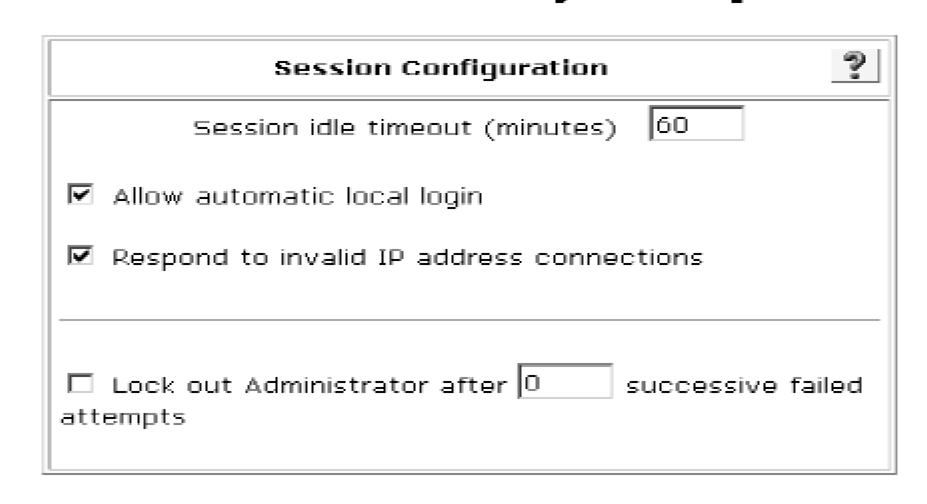


图 6-104　设置会话策略

❻ 单击 Audit Policy 可以设置审计属性，如图 6-105 所示。

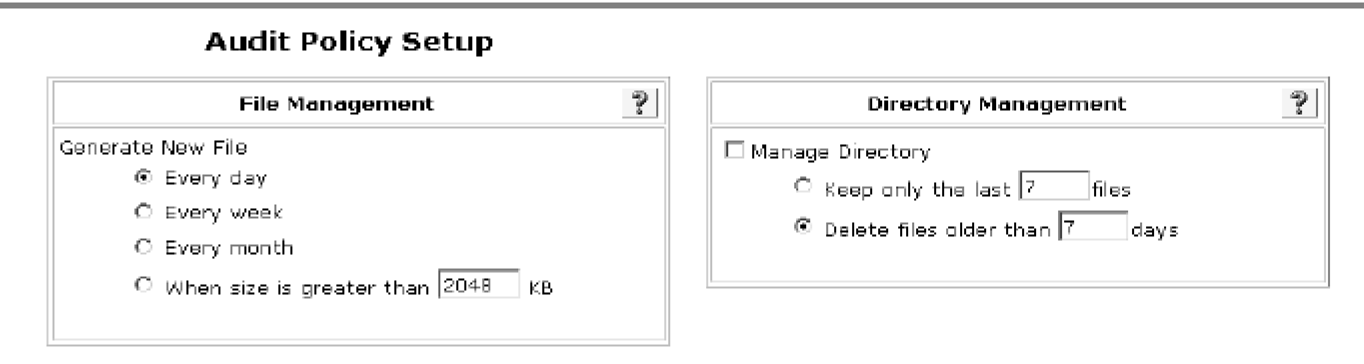


图 6-105　设置审计属性

❼ 完成以上设置后，在授权的 IP 地址上访问http://ACS-server-ip:2002/，并输入管理员账号远程登录 ACS，如图 6-106 所示。

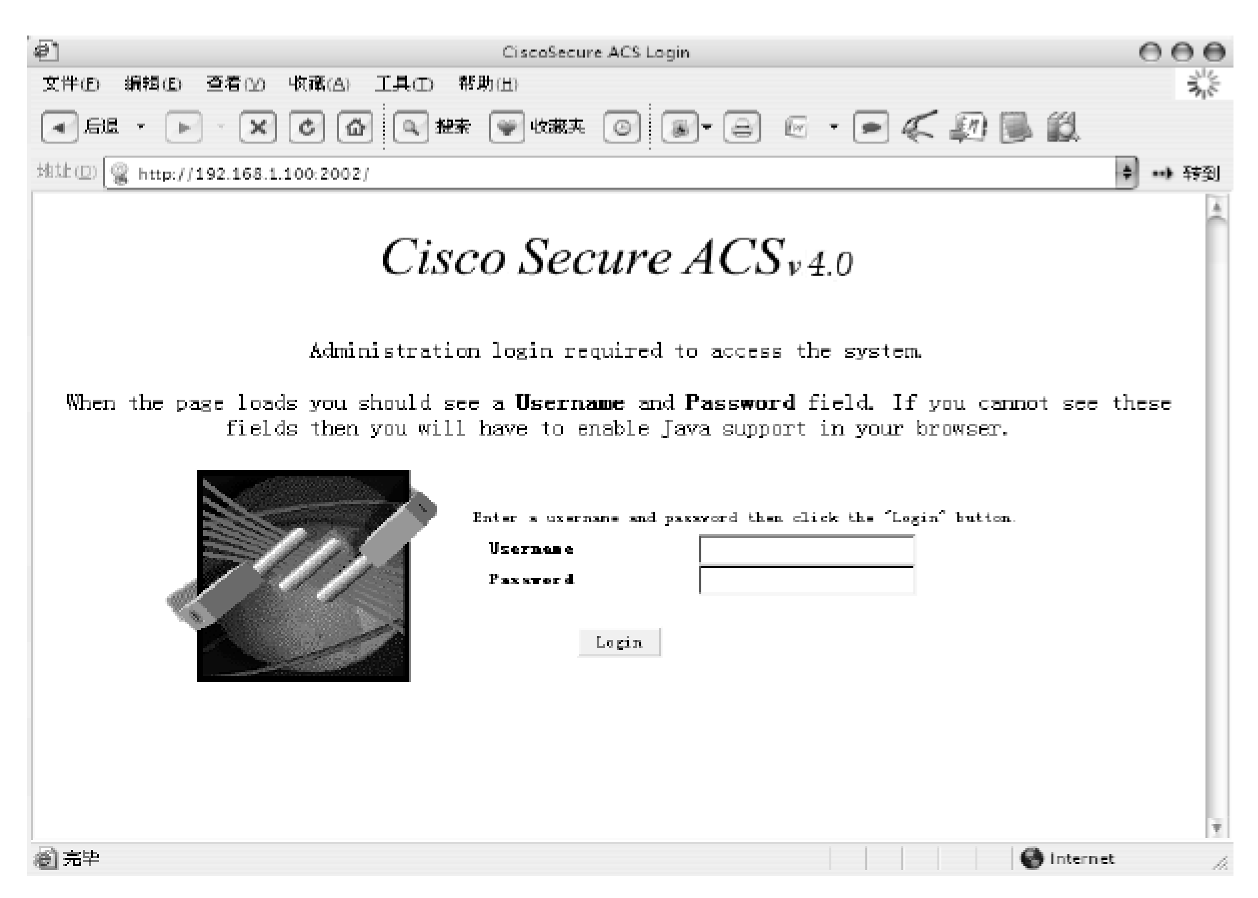


图 6-106　远程登录 ACS 界面

4. 添加/删除 AAA 客户端

对于一台基于 Cisco IOS 的路由器或者 NAS 接入服务器，若需要 Cisco Secure ACS 提供 RADIUS 认证，都将作为 Cisco Secure ACS 的 AAA 客户端。下面介绍添加/删除 AAA 客户端的过程。

❶ 在 ACS 主页面中，添加一个 AAA 客户端可以首先单击 Network Configuration 按钮，进入配置界面，再单击 Add Entry 按钮，打开 AAA 客户端管理界面，如图 6-107 所示。

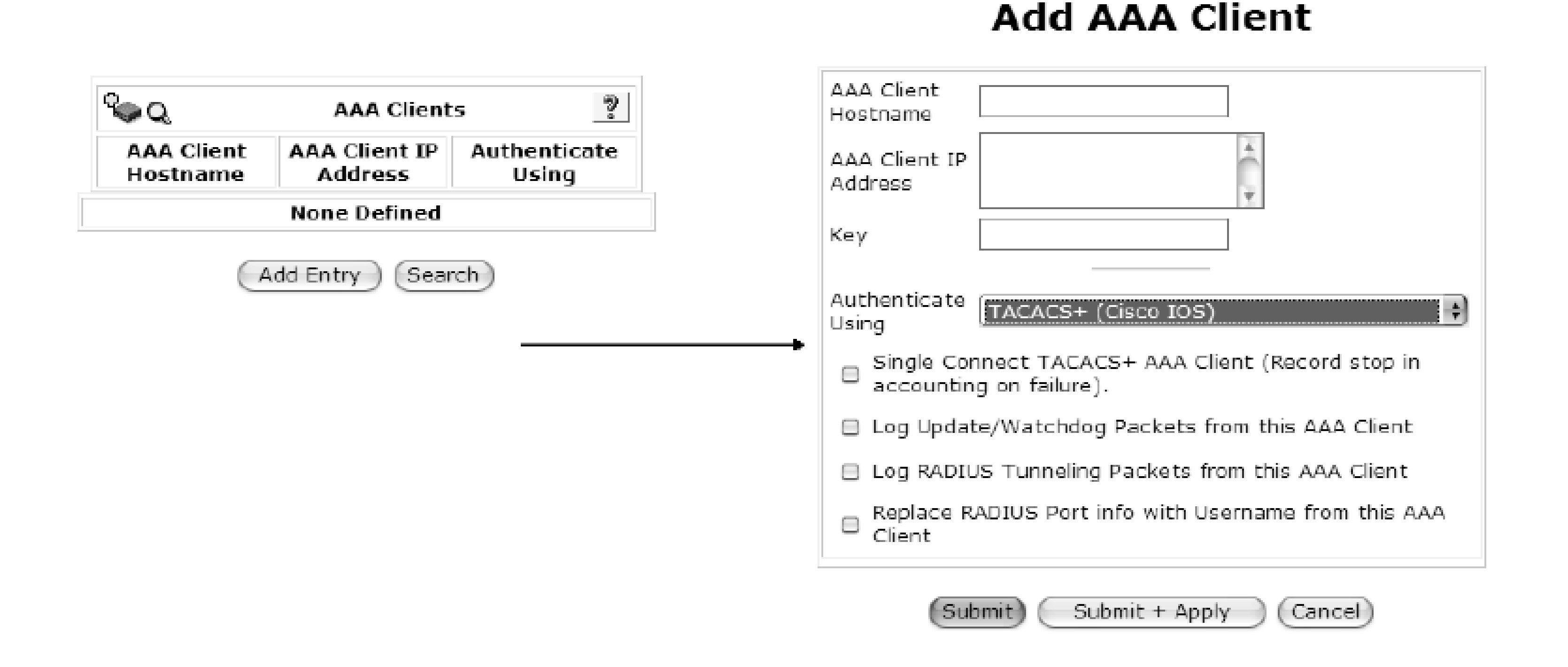


图 6-107　添加 AAA 客户端

❷ 在添加 AAA 客户端界面中可以定义客户端的主机名，并输入客户端的 IP 地址和 RADIUS 服务的密码。如果是配置一台基于 Cisco IOS 的路由器或者 NAS 接入服务器，则可以在下端的 Authenticate Using 中选择 RADIUS(Cisco IOS/PIX6.0)；如果是一些第三方设备，则可以选择 Radius(IETF)，然后单击 Submit+Apply 按钮。

❸ 修改成功后，会返回到 AAA 客户端管理界面，单击 AAA Client Hostname 可以继续修改先前的配置，或者删除该客户端。

5. 配置分布式 ACS

和前述的微软 IAS 定义 RADIUS 代理服务器的方法一样，Cisco Secure ACS 也支持分布式的运行模式，具体配置方式如下。

❶ 在 ACS 主页面中，单击 Interface Configuration 按钮，进入配置界面。在右侧单击 Advanced Options 选项，选中 Distribute System Settings 和 Network Device Group 两个复选框，然后单击 Submit 按钮，如图 6-108 所示。

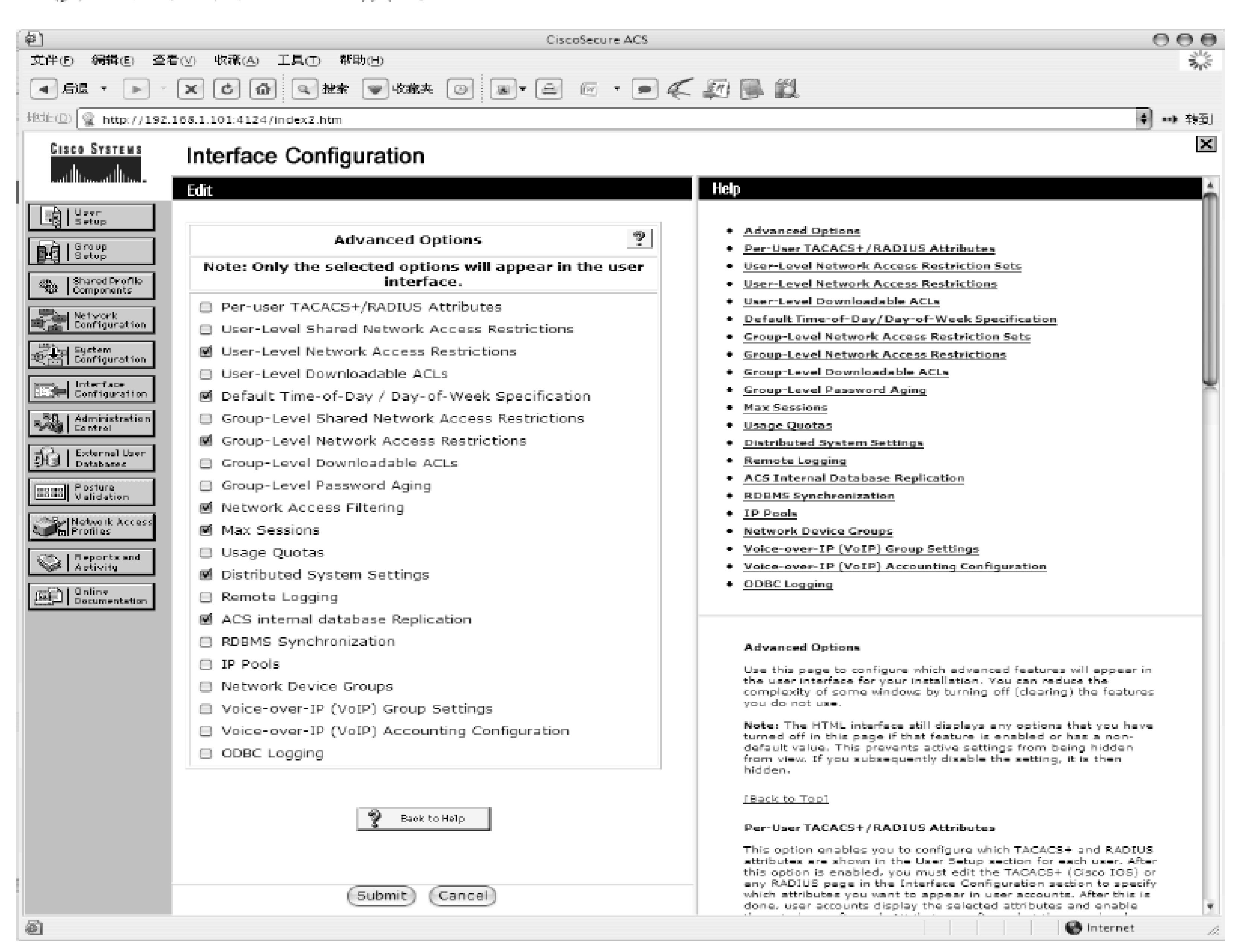


图 6-108　高级选项

❷ 单击 Network Configuration 按钮，进入配置界面，在右侧单击 Network Device Groups(NDG) 下方的 Add Entry 按钮，并在表中输入设备组的名称和密码，完成后单击 Submit 按钮，如图 6-109 所示。

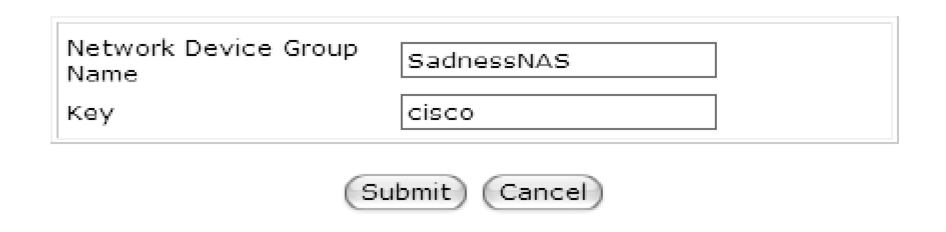


图 6-109　NDG 配置

❸ 回到 Network Configuration 配置界面，在右侧单击 Network Device Groups(NDG)下方的 Not Assigned 设备组，然后选择所需要迁移到新的 NDG 的 AAA Client 或者 AAA Server，如图 6-110 所示。

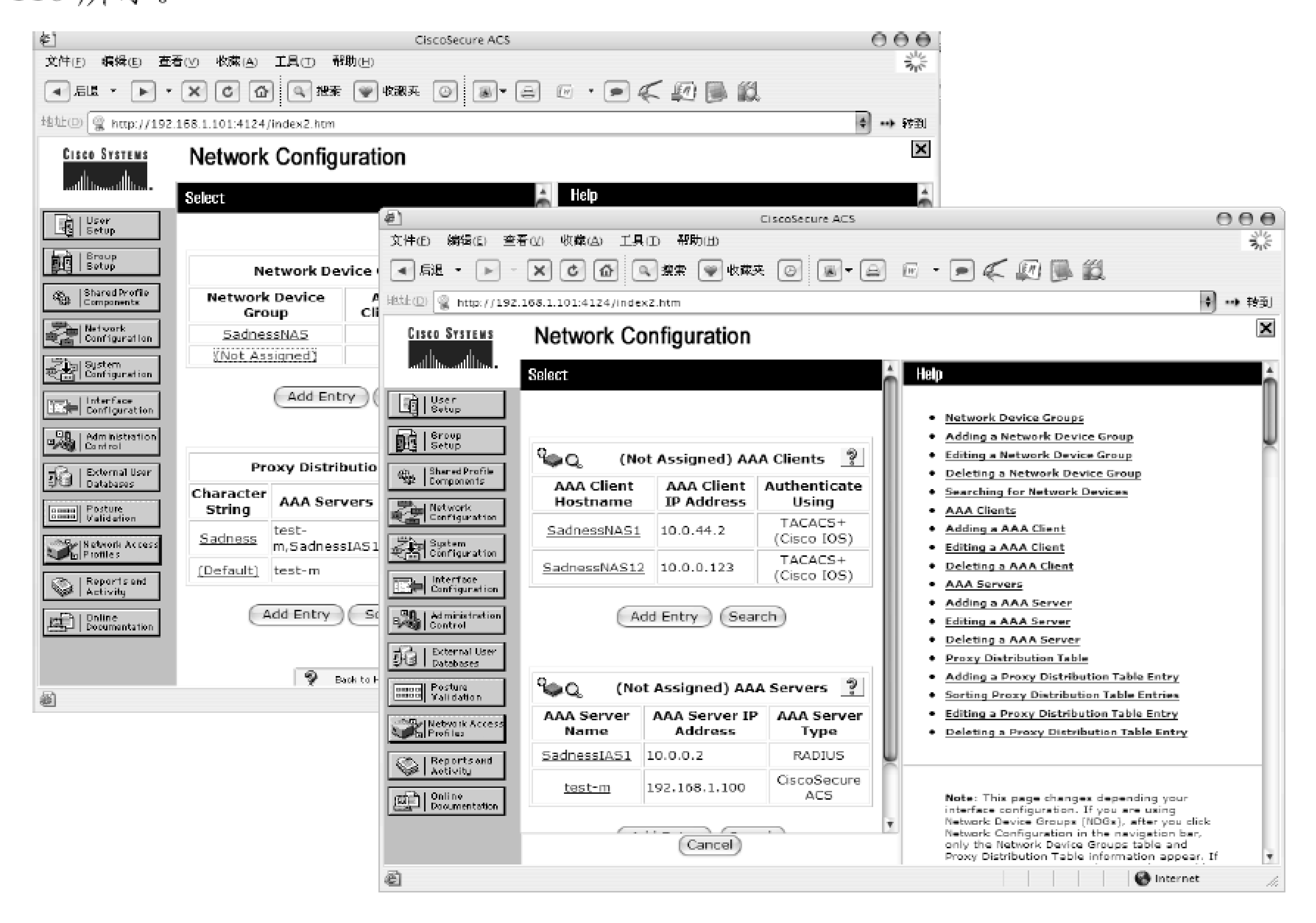


图 6-110 迁移设备到 NDG

❹ 在 Network Configuration 配置界面中，单击右侧 Network Device Groups(NDG)下方的 Not Assigned 设备组，然后选择所需要迁移到新的 NDG 的 AAA Client 或者 AAA Server，并在 Network Device Groups 下拉菜单中选择移动到新建的 Sadness NAS 组中，如图 6-111 所示。



图 6-111 迁移设备进入 NDG

❺ 在 Network Configuration 配置界面中，单击右侧 Proxy Distribution Table 下方的 Add Entry 按钮，输入这个转发列表的名称，并将 Position 设置为 Suffix，将需要的 RADIUS Server 加入 Forward To 一列，并选择记账方式为 Local/Remote，完成配置后单击 Submit+Restart 按钮，如图 6-112 所示。

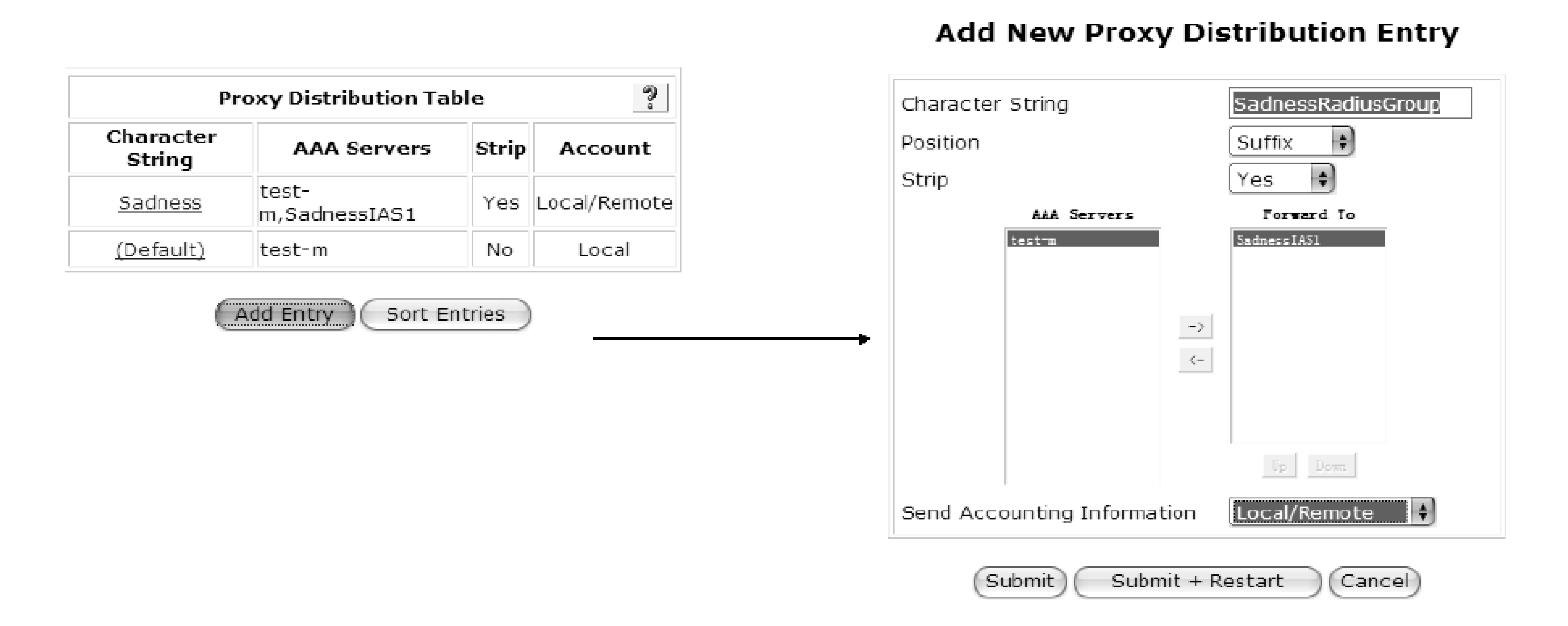


图 6-112　配置 Proxy Distribution Table

❻ 通常在多个 ACS 服务器之间需要进行数据同步，首先单击 Network Configuration 按钮，进入配置界面，在右侧单击 Advanced Options 选项，选中 RDBMS Synchronization。然后进入 System Configuration，选择 RDBMS Synchronization ，如图 6-113 所示。

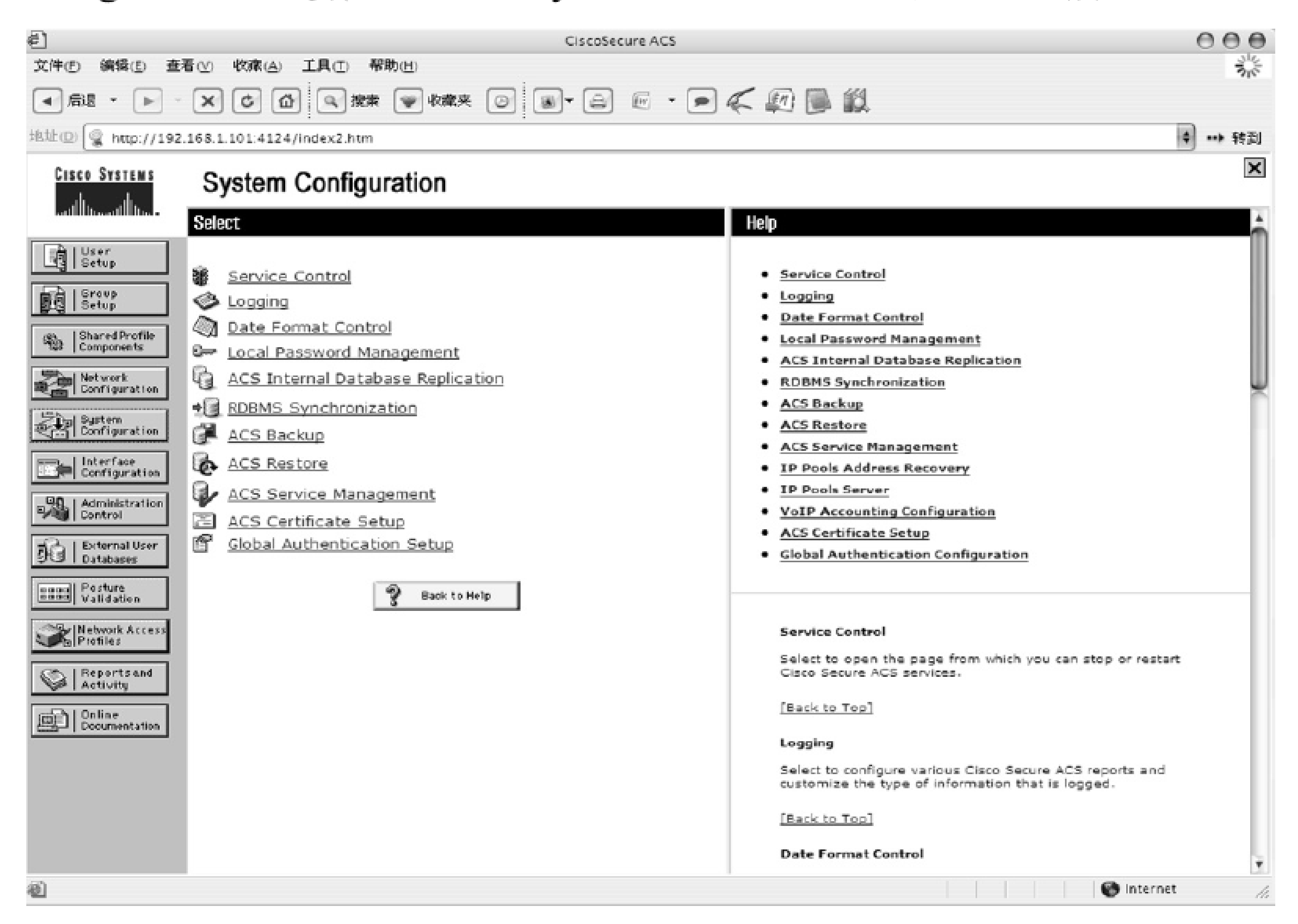


图 6-113　配置 RDBMS Synchronization

❼ 在新弹出的 RDBMS Setup 页面中可以设置数据源，以及用于同步的用户名和密码。Synchronization Scheduling 可以选择同步的周期，并允许在每天的特定时间进行同步以避开业务高峰期等。最后设置 Synchronization Partners，这里可以选择不同的 Secure ACS 服务器

进行同步，如图 6-114 所示。

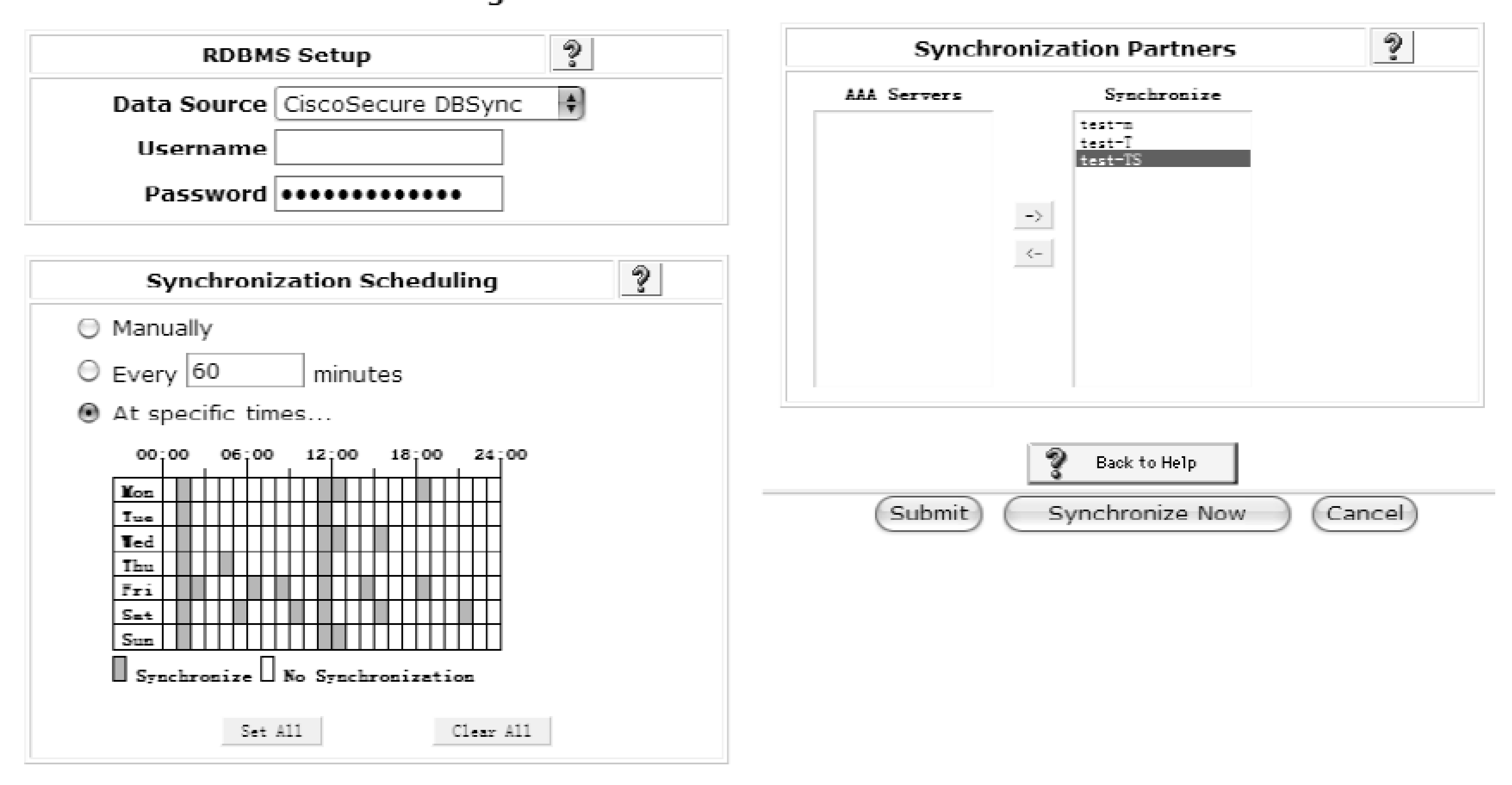


图 6-114　配置 RDBMS Synchronization Setup

6. 添加 RADIUS 用户

添加 RADIUS 用户用于 AAA 认证，通常可以选择 External User Databases 按钮来使用 Windows Active Directory 的账号。更多情况下，Cisco Secure ACS 还是使用自带的用户设置功能，其配置方法如下。

❶ 在 ACS 主页面中，首先单击 User Setup 按钮，进入用户配置界面。再在右侧的文本框中输入需要添加的用户名，并单击 Add/Edit 按钮，如图 6-115 所示。

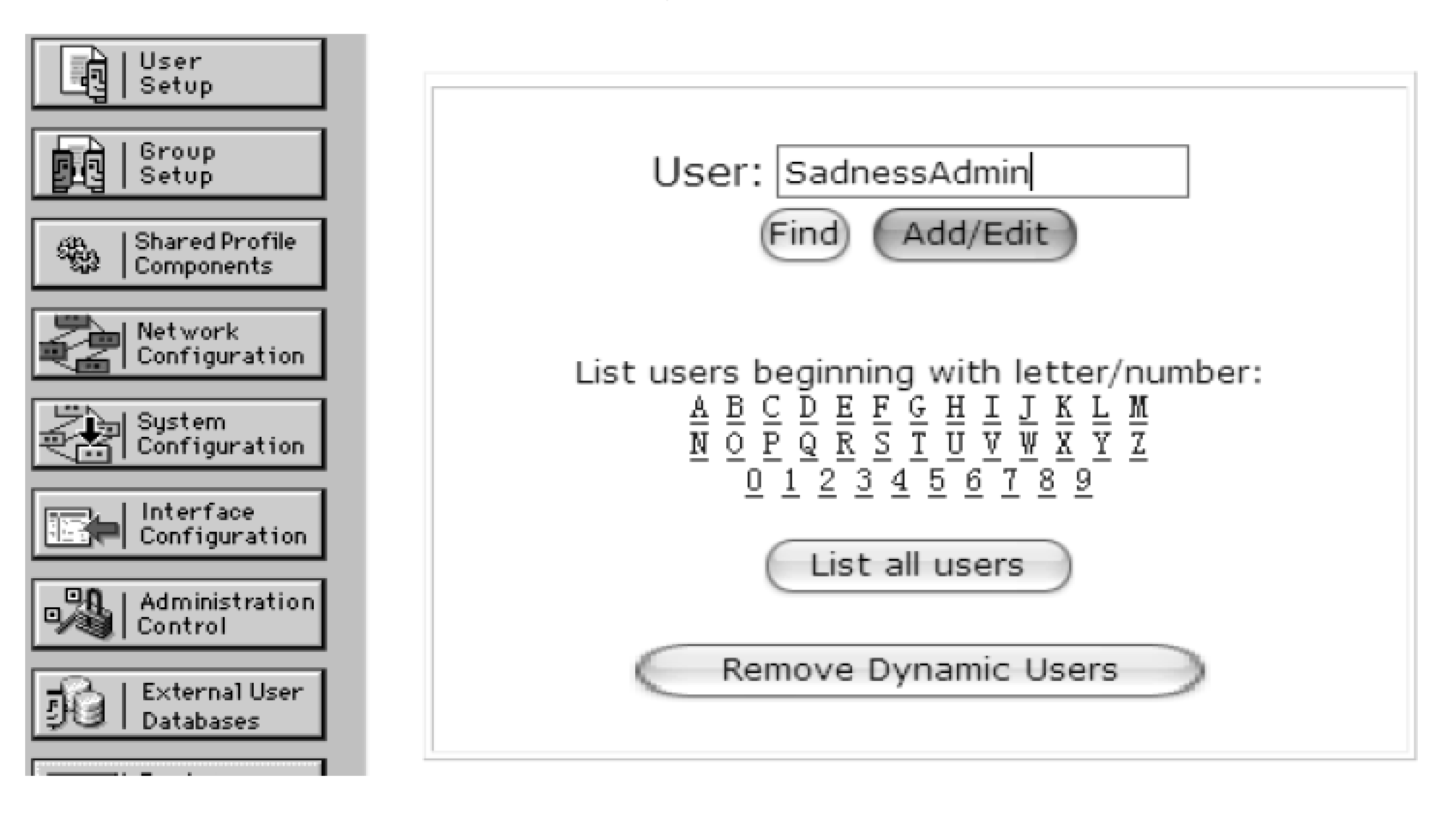


图 6-115　输入 RADIUS 用户名

❷ 设置用户的真实名字、详细描述等信息。在 User Setup 界面中可以定义认证密码使用 ACS 的内部数据库或者 Windows 的用户数据库，然后设置 PAP 或者 CHAP 的密码；选择相应的用户组，还可以设置 Callback 以及用户账号有效期等权限、详细列表，如图 6-116 所示。

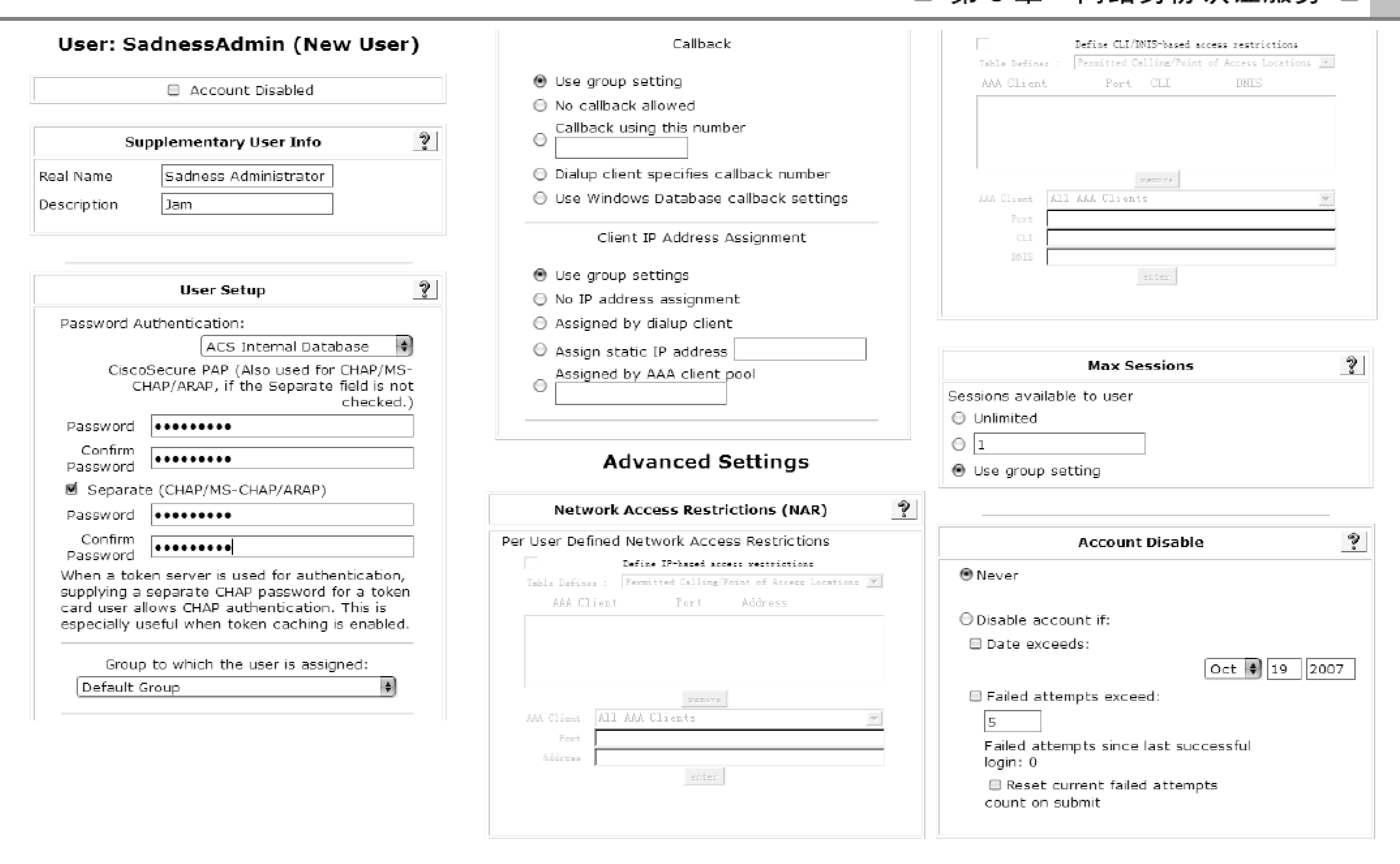


图 6-116　设置 RADIUS 用户详细信息

❸ 完成配置后单击 Submit 按钮，单击 Group Setup 按钮后找到刚才账号所在的组并单击 Edit Settings 按钮，可以配置该组用户的接入时间；如果是配置 TACACS+还可以定义用户的权限，然后定义用户的最大接入会话数量。RADIUS 用户还可以定义权限 Level，如图 6-117 所示。

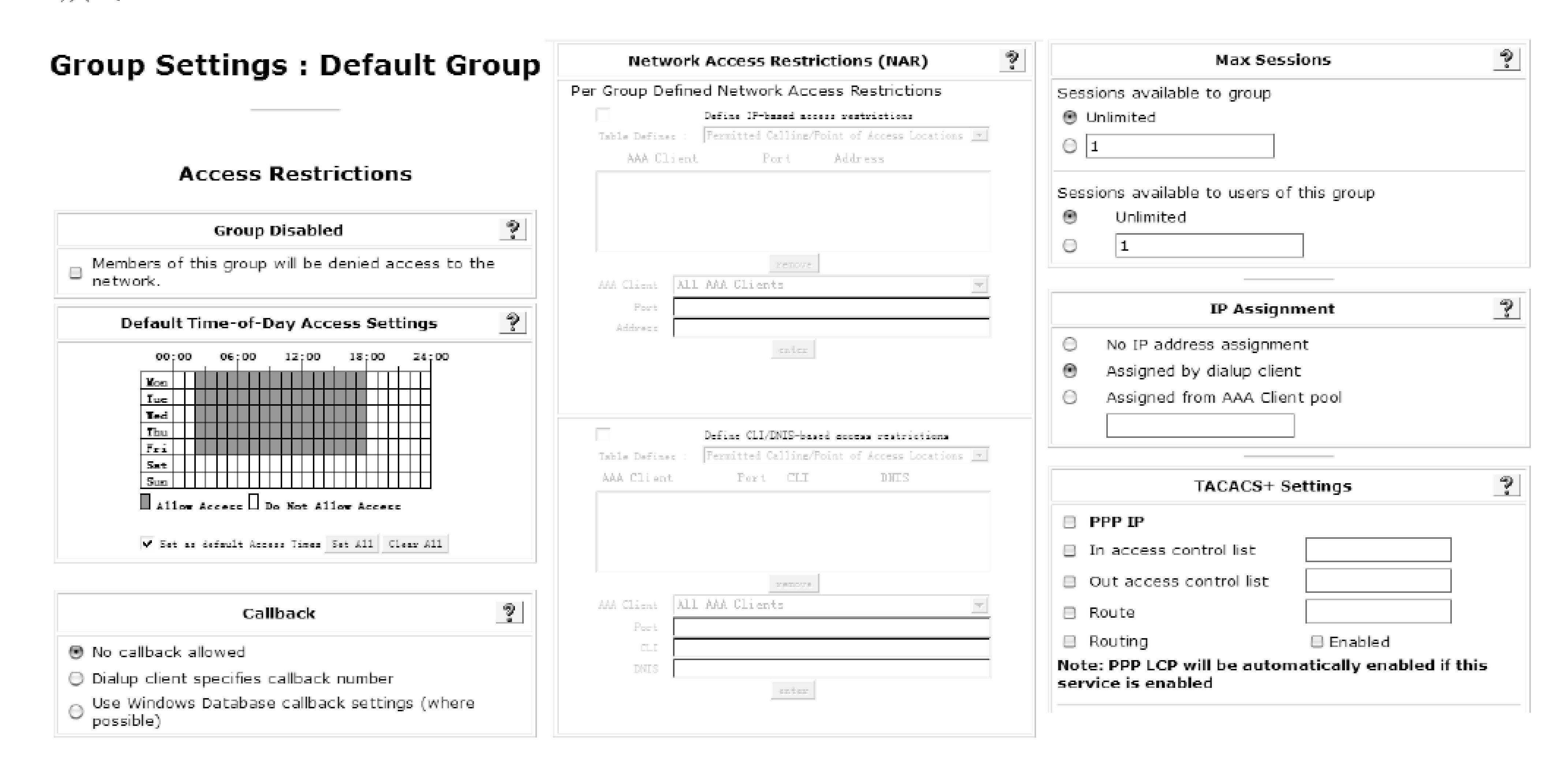


图 6-117　其他配置

❹ 完成配置后单击 Submit 按钮。

7. 授权及审计配置

下面简要地介绍一下授权及审计的配置，限于篇幅，这里就不详细介绍配置方法。

❶ 授权通常在 Shared Profile Components 菜单中设置，可以定义 RADIUS 以及 Shell Command 等权限，如图 6-118 所示。

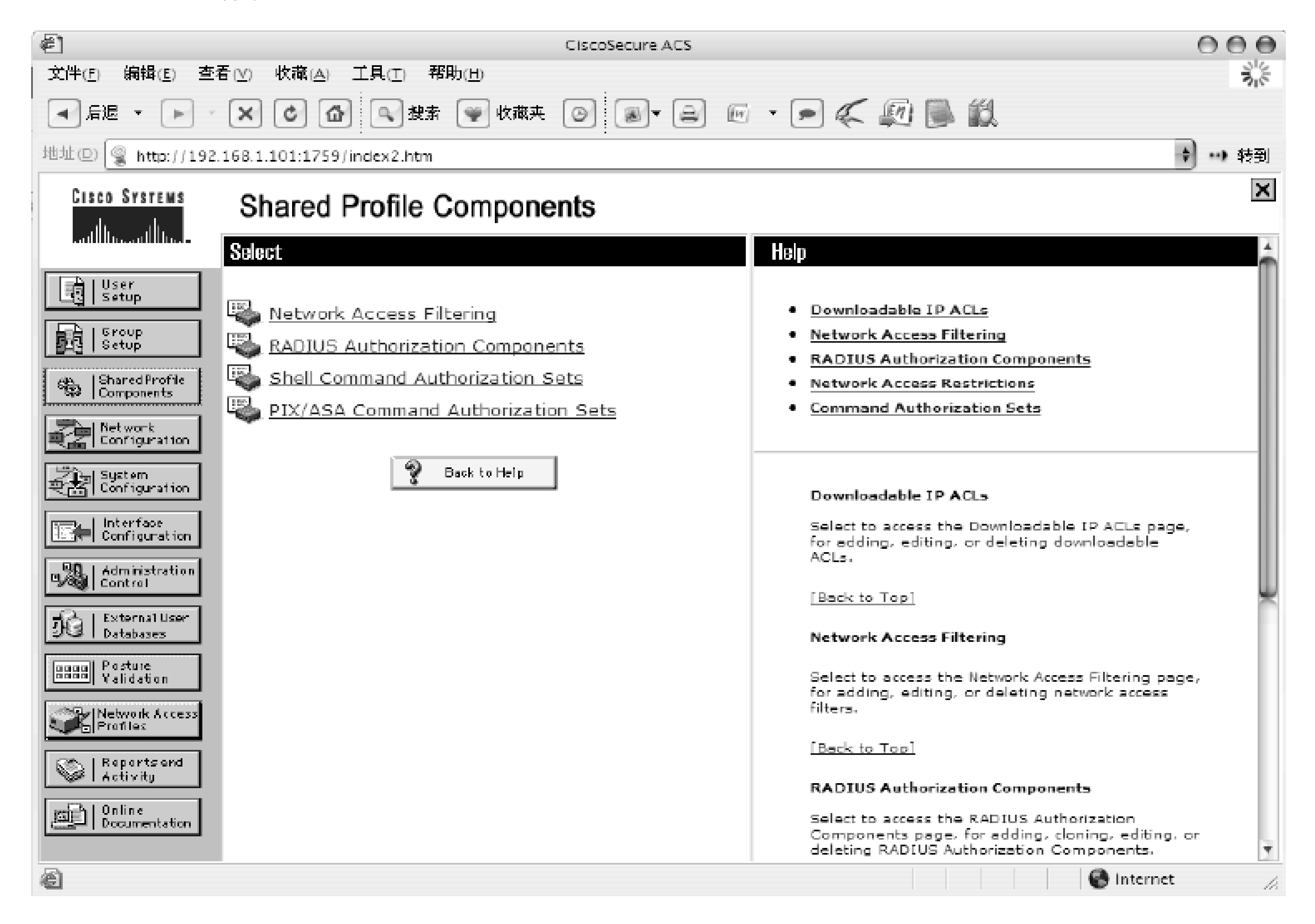


图 6-118　配置授权

❷ 对于审计服务，可以在 Reports and Activity 中查询，如图 6-119 所示。

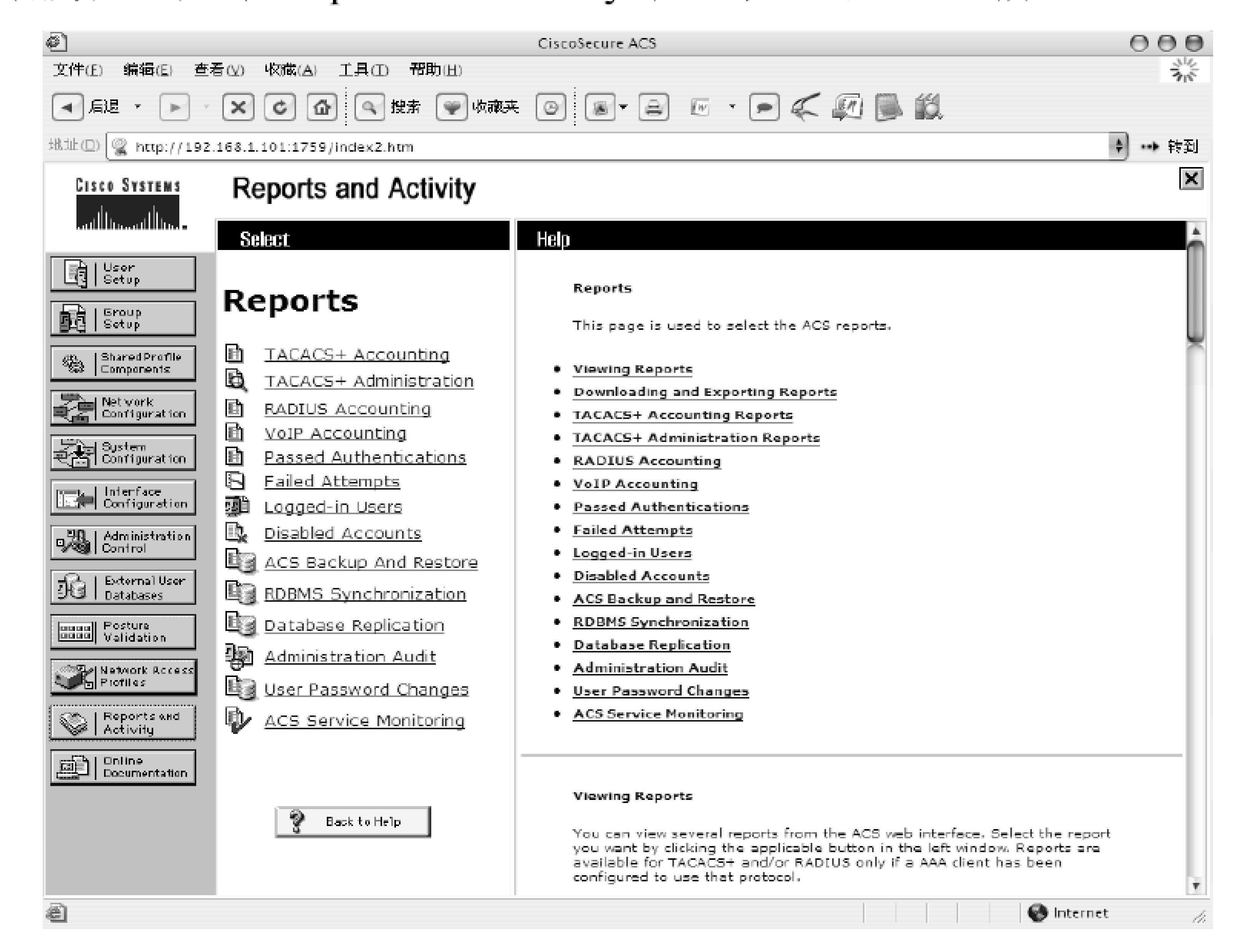


图 6-119　查看审计

6.3.4　Linux RADIUS

对于中小型企业 NAS 应用来说，以 Linux 为平台建立 RADIUS 服务器是非常好的选择。使用共享软件完全可以建立简洁、高效的 RADIUS 服务器，而且无须任何软件上的花费。在目前很多较高版本的 Linux 中，它们都把 RADIUS 的安装程序包含在系统源码中，这样使得我们可以很容易地通过免费的 Linux 系统学习 RADIUS 授权、认证的原理和应用。

在 Linux 下安装 RADIUS Server，通常使用的是 IC-RADIUS，它需要如下软件包的支持。

- ✧ mysql-3.23.39.tar.gz:　MySQL 数据库；
- ✧ DBI-1.18.tar.gz:　Perl 调用数据库的通用接口；
- ✧ Msql-Mysql-modules-1.2216.tar.gz:　Perl DBI 针对 MySQL 的 Driver 驱动；
- ✧ RadiusPerl-1.05.tar.gz:　Perl 对 RADIUS 的 Authen 认证模块；
- ✧ icradius-0.18.1.tar.gz:　IC-RADIUS 源码包。

下面是在 Linux 下安装 RADIUS Server 的一般过程，不同版本的 Linux 的方法可能不同。

❶ 安装 MySQL 数据库管理系统。不同版本的安装方法不尽相同(下同)，下面所列的是下载源代码的安装过程。

```
SadnessNet#gzip zxvf mysql-3.23.39.tar.gz      //解压缩
SadnessNet#cd mysql-3.23.39
SadnessNet#./configure prefix=/usr/local/mysql     //配置MySQL的安装路径
SadnessNet#make                                //编译
SadnessNet#make install                        //安装
SadnessNet#cd /usr/local/msyql/bin
SadnessNet#./mysql_install_db                  //初始化MySQL数据库
SadnessNet#ldconfig                            //更新系统共享库链接
SadnessNet#cd /usr/tmp/mysql-3.23.39/support-files
SadnessNet#cp mysql.server  /etc/rc.d/init.d/mysql.server//复制启动/停止脚本
SadnessNet#cp my-medium.cnf  /etc/my.cnf       //复制配置文件，并修改my.cnf 中
                                                 root密码为空
SadnessNet#mysqladmin u root p password        //新口令
```

❷ 安装 Perl 调用数据库的通用接口 DBI 及 DBD for MySQL 驱动。

```
SadnessNet#cd /usr/tmp
SadnessNet#tar zxvf DBI-1.18.tar.gz
SadnessNet#cd DBI-1.18
SadnessNet#perl Makefile.PL
SadnessNet#make test
SadnessNet#make install
SadnessNet#cd /usr/tmp
SadnessNet#tar zxvf Msql-Mysql-modules-1.2216.tar.gz
SadnessNet#cd Msql-Mysql-modules-1.2216
SadnessNet#perl Makefile.PL'
SadnessNet#make
SadnessNet#make test
SadnessNet#make install
```

❸ Perl 对 RADIUS 的认证模块安装 RADIUSPerl:Authen。

```
SadnessNet#cd /usr/tmp
SadnessNet#tar zxvf RadiusPerl-0.05.tar.gz
SadnessNet#cd RadiusPerl-0.05
SadnessNet#perl Makefile.PL
SadnessNet#make
SadnessNet#make test
SadnessNet#make install
```

❹ 安装 RADIUS 服务器软件 IC-RADIUS。

```
SadnessNet#cd /usr/tmp
SadnessNet#tar zxvf icradius-0.18.1.tar.gz
SadnessNet#cd icradius-0.18.1
SadnessNet#cp Makefile.lnx Makefile
SadnessNet#make
SadnessNet#make install
```

❺ 安装完成 RADIUS 服务器软件后，需要配置 RADIUS 数据库，并向 MYSQL 数据库中导入数据表。

```
SadnessNet#cd scripts
SadnessNet#mysql u root p mysql
Mysql>create database radius; //创建RADIUS数据库
添加RADIUS用户:
Mysql>grant all on radius.* on radius@localhost identified by 'radius';
SadnessNet#mysqladmin u root p refresh //刷新数据库内容
```

导入数据表:

```
SadnessNet# mysql -u root -pyourpassword radius < radius.db
```

修改 dictimport.pl，设置

```
my $dbusername = 'radius';
my $dbpassword = 'radius'
SadnessNet# ./dictimport.pl ../raddb/dictionary
```

❻ 上述软件安装完成后，便可启动 RADIUS 服务。

```
SadnessNet#cd /etc/rc.d/init.d
SadnessNet#radiusd start
```

6.4 本章小结

本章介绍了关于网络认证的一些服务，首先介绍了基于 Windows 电子证书系统的安装和配置流程。在后续的小节中介绍了如何使用 AAA 来管理大量的设备，以及如何对这些设备进行身份验证、授权访问以及事后审计等功能。

接下来介绍了基于 RADIUS 服务器的 AAA 方案，并分别介绍了微软 IAS 系统、Cisco Secure ACS 以及基于 Linux 的 IC-RADIUS 等的安装和配置。微软 IAS 系统由于和微软产品结合非常紧密，所以在 Active Directory 大规模部署的平台上可以很好地支持 AAA 服务。而 Cisco Secure ACS 产品由于出自专业的通信设备厂商、系统稳定性以及和其他基于 Cisco 的

网络设备互动性能做得更加出色，并且其私有的 TACACS+协议也支持很多特有的功能，并且它还可以通过外部数据库共享 Active Directory 中的用户数据。IC-RADIUS 是一个完全免费的解决方案，它非常适合那些需要安全性的中小型企业使用，这也是我们介绍基于 Linux RADIUS 服务器的初衷。

在第 7 章中，我们将逐渐开始使用这些服务进行 802.1x 以及网络接入控制(NAC)的配置。

第 7 章　网络安全接入

目前，大量的网络安全威胁来自于各种蠕虫和木马。蠕虫、木马等形式的病毒对网络的威胁极大，通过主机间的相互传染使得网络安全性极度下降，因此需要一种技术将安全的计算机放入受保护的区域，并对中毒的主机进行有效的隔离，防止其扩散感染其他主机。

通过本章的学习，读者应掌握以下主要内容：

✧ 802.1x 接入认证
✧ WSUS windows 自动更新服务
✧ Cisco NAC 网络准入控制
✧ 终端安全

7.1　802.1x 协议

7.1.1　802.1x 协议概述

802.1x 协议是基于 Client/Server 的访问控制和认证协议，用来限制未经授权的用户/设备通过接入端口访问 LAN/MAN。在获得交换机或 LAN 提供的各种业务之前，802.1x 协议对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1x 协议只允许 EAPoL(Extensible Authentication Protocol over LAN，基于局域网的扩展认证协议)数据通过设备连接的交换机端口，认证通过以后，正常的数据可以顺利地通过以太网端口。

网络访问技术的核心部分是 PAE(Port Access Entity，端口访问实体)。在访问控制流程中，端口访问实体包含三部分。

✧ 认证者：对接入的用户/设备进行认证的端口；
✧ 请求者：被认证的用户/设备；
✧ 认证服务器：根据认证者的信息，对请求访问网络资源的用户/设备进行实际认证功能的设备。

以太网的每个物理端口分为受控和不受控两个逻辑端口，物理端口收到的每个帧都被送到受控和不受控端口。对受控端口的访问，受限于受控端口的授权状态。认证者的 PAE 根据认证服务器认证过程的结果，控制“受控端口”的授权/未授权状态。处在未授权状态的控制端口将拒绝用户/设备的访问。

1. 802.1x 协议认证特点

基于以太网端口认证的 802.1x 协议具有如下特点。

✧ 802.1x 协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有

效降低建网成本。

✧ 借用了在 RAS 系统中常用的 EAP(扩展认证协议)，可以提供良好的扩展性和适应性，实现对传统 PPP 认证架构的兼容。
✧ 802.1x 协议的认证体系结构采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离，由 RADIUS 和交换机利用不可控逻辑端口共同完成对用户的认证与控制，业务报文直接承载在正常的二层报文上通过可控端口进行交换，通过认证后的数据包是无须封装的纯数据包。
✧ 可以使用现有的后台认证系统降低部署的成本，而且有丰富的业务支持；可以映射不同的用户认证等级到不同的 VLAN。
✧ 可以使交换端口和无线 LAN 具有安全的认证接入功能。

2. 802.1x 协议工作过程

图 7-1 所示的是 802.1x 协议的工作流程。

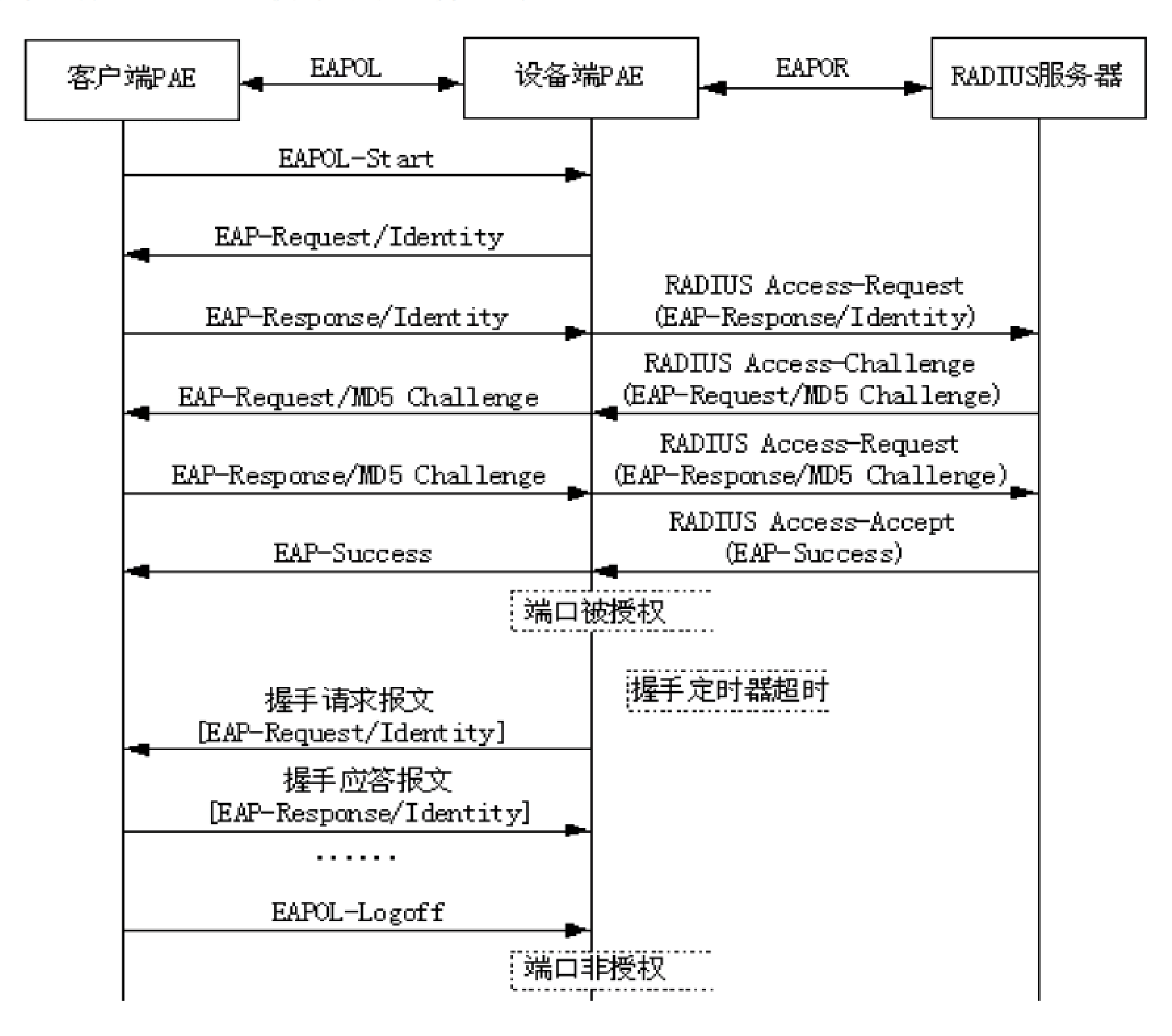


图 7-1　802.1x 工作流程

(1)　当用户有上网需求时打开 802.1x 协议客户端程序，输入已经申请、登记的用户名和口令，发送连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

(2)　交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名发送过来。

(3)　客户端程序响应交换机发出的请求，将用户名信息通过数据帧发送给交换机。同时，交换机将客户端送上来的数据帧经过封包处理后发送给认证服务器进行处理。

(4)　认证服务器收到交换机转发的用户名信息后，将该信息与数据库中的用户名列表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

(5)　客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理(此种加密算法通常是不可逆的)，并通过交换机传给认证服务器。

(6)　认证服务器将送上来的加密后的口令信息与其自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息并向交换机发出打开端口的指令，允许用户的业务流通过端口访问网络；否则，反馈认证失败的消息并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

3. 802.1x 应用环境特点

802.1x 既可应用于交换式以太网络环境，也可应用于共享式网络环境。

1)　交换式以太网络环境

在交换式以太网络中，用户和网络之间采用点到点的物理连接，用户彼此之间通过 VLAN 隔离。在这种网络环境下，网络管理控制的关键是用户接入控制，802.1x 不需要提供过多的安全机制。

2)　共享式网络环境

当 802.1x 应用于共享式的网络环境时，为了防止在共享式的网络环境中出现类似“搭载”的问题，有必要将 PAE 实体由物理端口进一步扩展为多个互相独立的逻辑端口。逻辑端口和用户/设备形成一一对应关系，并且各逻辑端口之间的认证过程和结果相互独立。在共享式网络中，用户之间共享接入物理媒介，接入网络的管理控制必须兼顾用户接入控制和用户数据安全，可以采用的安全措施是对 EAPoL 和用户的其他数据进行加密封装。在实际网络环境中，可以通过加速 WEP 密钥重分配周期，弥补 WEP 静态分配密钥导致的安全性缺陷。

7.1.2　配置 802.1x 协议

应用实例导航：为 Sadness 公司部署基于 802.1x 接入控制

※场景呈现

Jam 为了使 Sadness 公司的网络更加安全，并随着公司内部无线网络的部署，为了防止陌生人接入网络，他在公司采用了 802.1x 认证。

项目实施后，虽然安全性进一步提高了，但是公司不少员工抱怨，使用两套密码进行 Windows 登录和 802.1x 认证非常麻烦，管理维护成本也较高，希望使用新的配置进行单一账号的身份认证。在现阶段，通常使用 Windows Active Directory 和 Cisco Secure ACS 结合来完成统一账号的登录服务。

※技术要领

(1) 配置 Active Directory，实现单一账号身份认证；
(2) 配置 RADIUS 服务器；
(3) 在网络接入设备上，启用 802.1x；
(4) 配置 802.1x 客户端。

1. 配置 Active Directory

在上一章，已经介绍了 Active Directory 的安装过程，为了使用户能够使用单一账号的身份认证，需要对 Active Directory 进行一些必要的配置，其过程如下。

❶ 以 Administrator(系统管理员)身份登录域控制器，依次单击【开始】→【管理工具】→【Active Directory 用户和计算机】命令，打开【Active Directory 用户和计算机】控制台窗口，在左侧窗格中用鼠标右键单击域名，在弹出的快捷菜单中选择【新建】→【组织单位】命令。在弹出的【新建对象-组织单位】对话框中输入组织单位的名称为 dot1x，并单击【确定】按钮，如图 7-2 所示。



图 7-2 添加组织单位的名称

❷ 在 Users 结点中选择需要添加到刚才所建 dot1x 组织单位的用户，然后右击，在弹出的快捷菜单中选择【移动】命令，将这些用户移动到 dot1x 组织单位中，如图 7-3 所示。

❸ 选择刚才所建的组织单位，右击，在弹出的快捷菜单中选择【委派控制】命令，弹出【控制委派向导】对话框，单击【下一步】按钮，如图 7-4 所示。

❹ 在【用户和组】向导页中，选择新建的组织单位的用户，单击【下一步】按钮，打开【要委派的任务】向导页。在【要委派的任务】向导页的【委派下列常见任务】列表框中，列出了可以委派的任务列表，选中【重设用户密码并强制在下次登录时更改密码】复选框，单击【下一步】按钮，如图 7-5 所示。完成后再单击【下一步】按钮即可

完成配置。

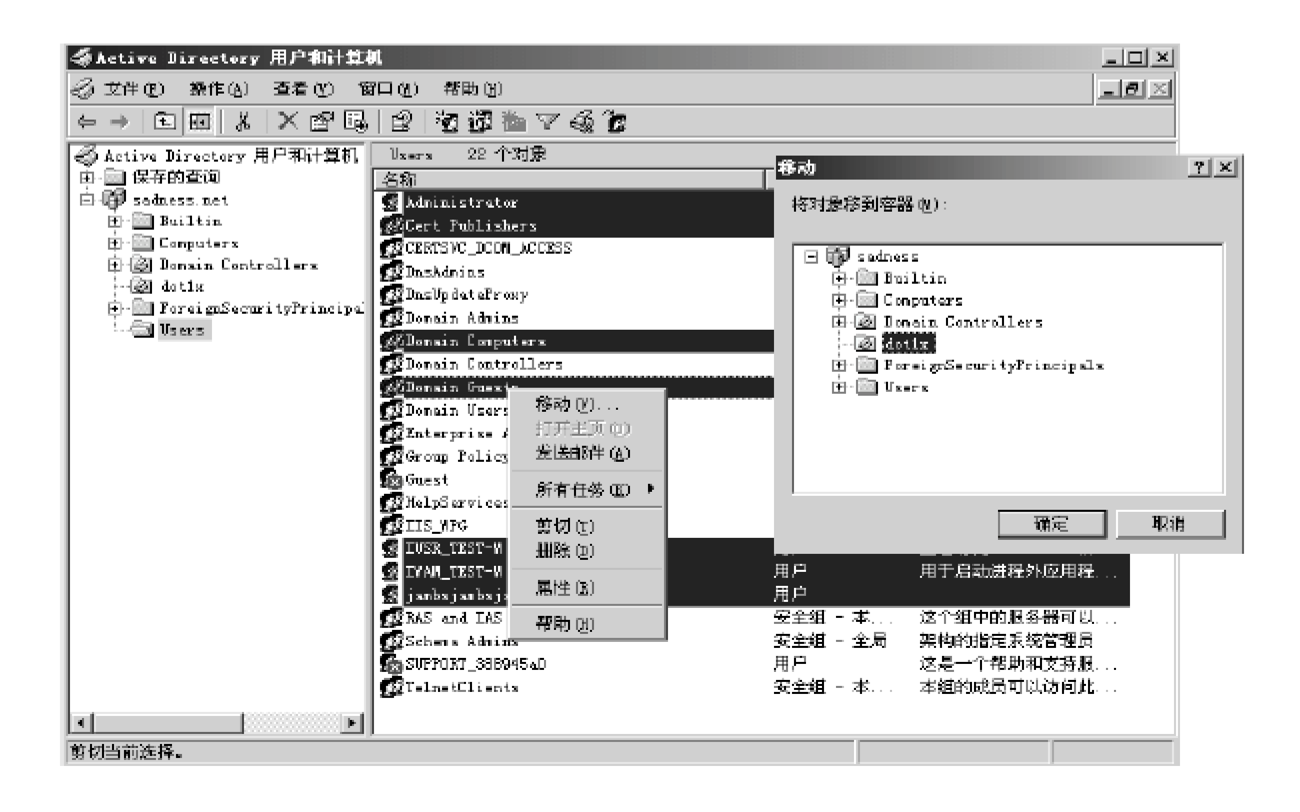


图 7-3　移动用户到自定义的组织单位中

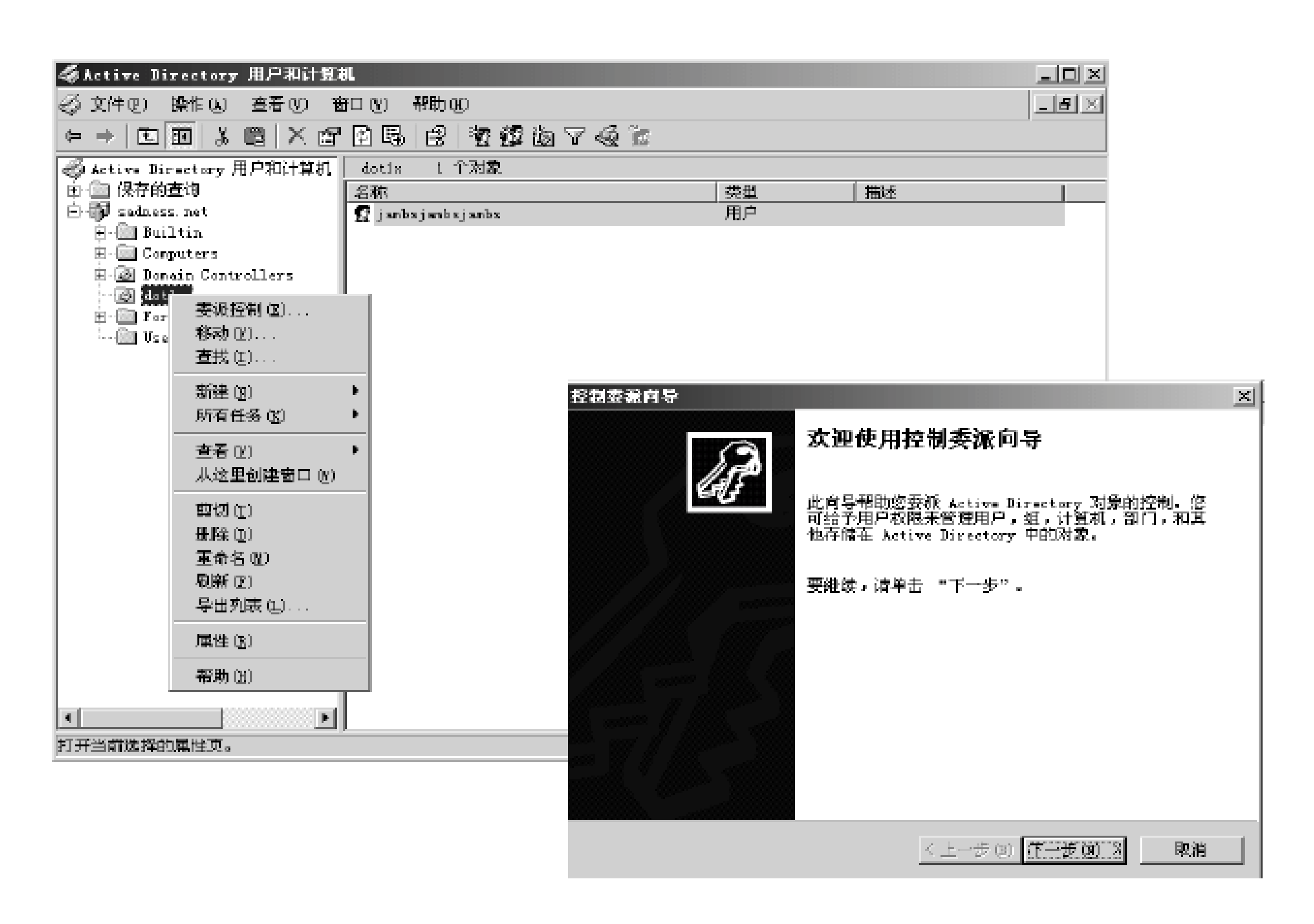


图 7-4　委派控制向导



图 7-5　选择委派任务

❺ 打开浏览器，在地址栏中输入“http://CA-server-ip/certsrv”，依次单击【申请一个证书】→【高级申请】→【创建并向此 CA 提交一个申请】链接，如图 7-6 所示。

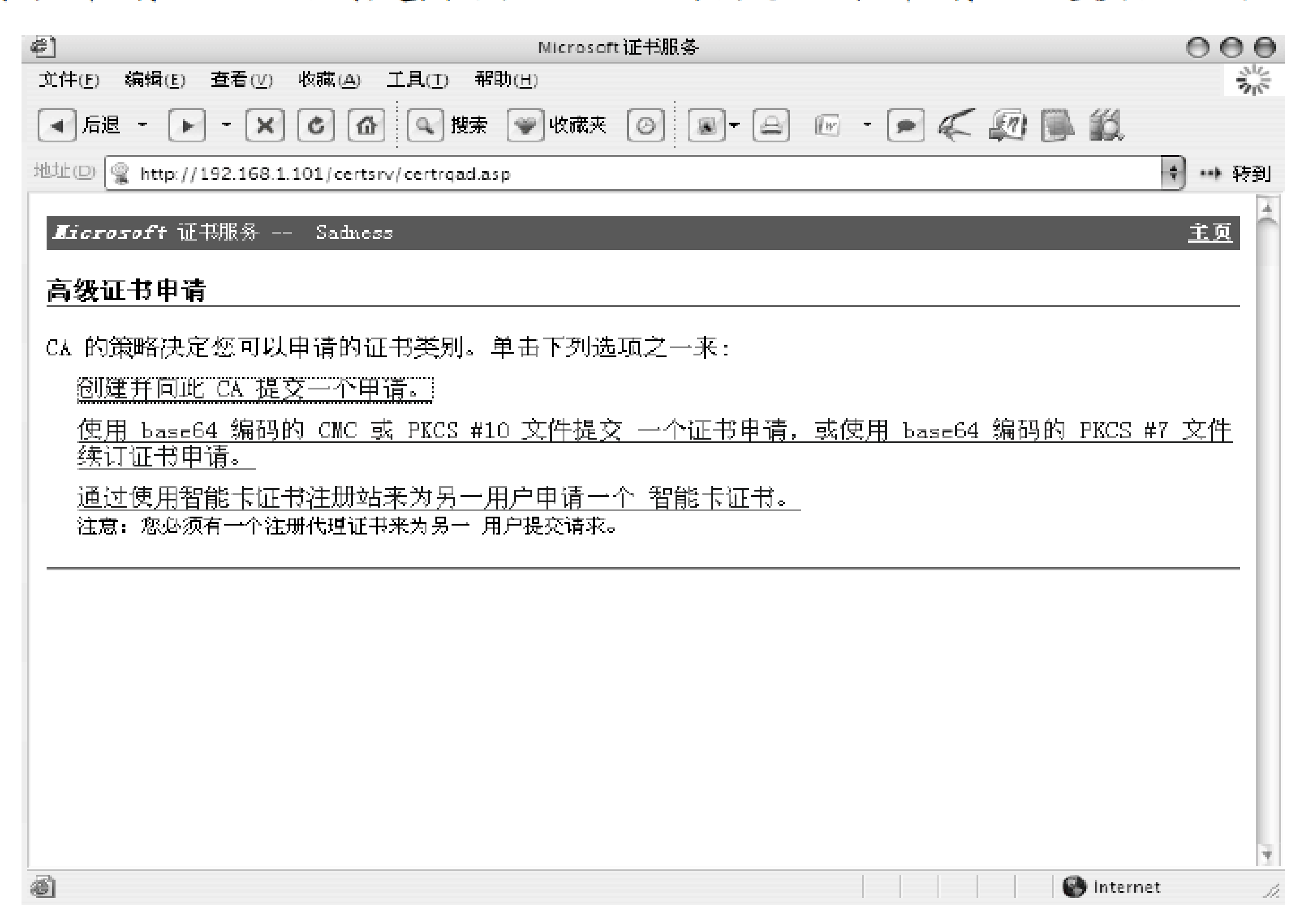


图 7-6 申请 CA 证书

❻ 在【高级证书申请】Web 页面中，在【证书模板】下拉列表框中选择【Web 服务器】选项，在【姓名】文本框中输入“Sadness”，在【密钥大小】文本框中输入“1024”，同时选中【标记密钥为可导出】及【将证书保存在本地计算机存储中】两个复选框，然后单击【提交】按钮，如图 7-7 所示。这时将打开【证书安装】的提示对话框，说明安装已经完成。

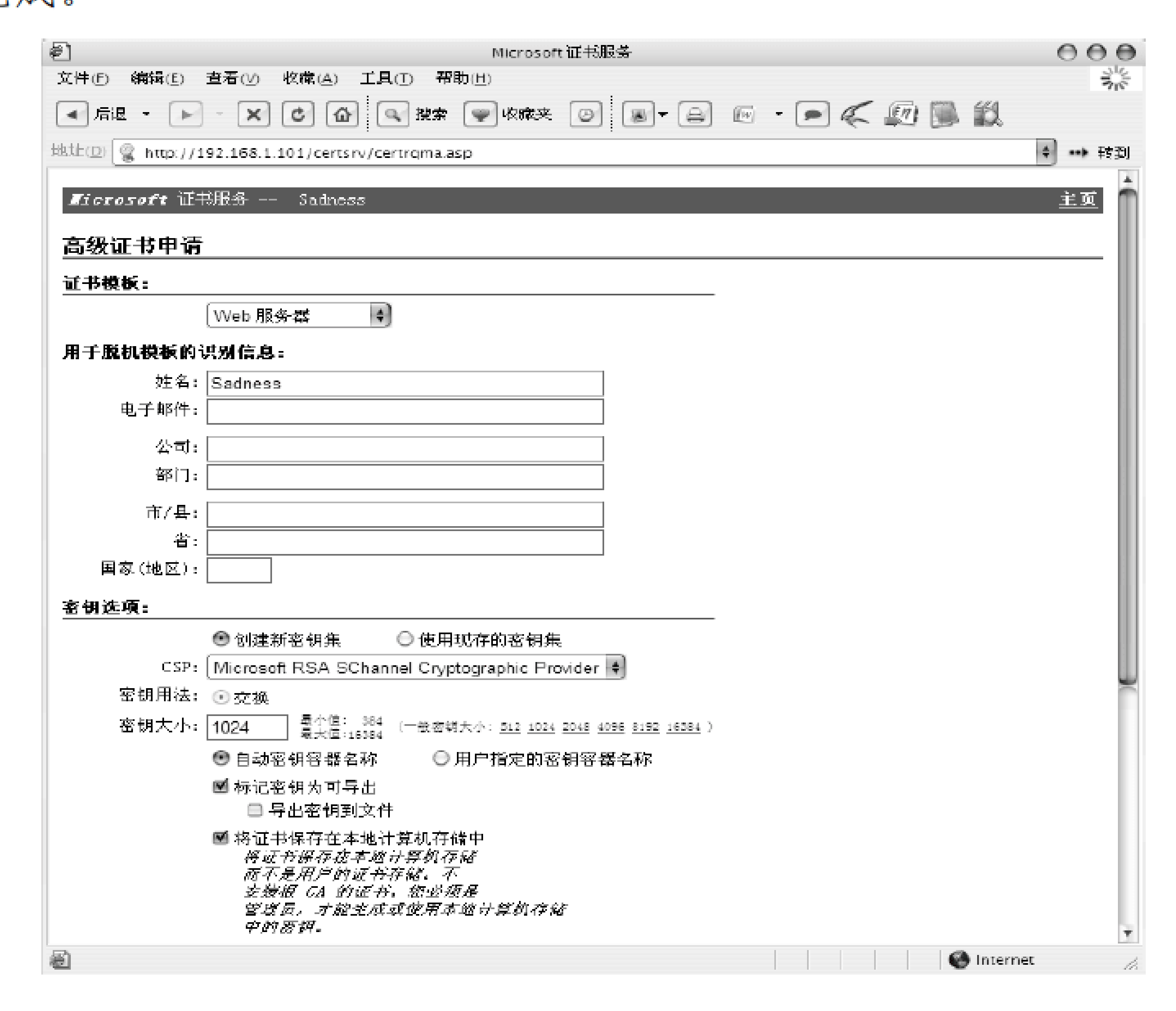


图 7-7 设置证书模板及密钥

2. 配置 RADIUS 服务器

采用 802.1x 认证时，用户认证过程使用 RADIUS 协议，网络接入设备(交换机或 AP)都是 RADIUS 客户端。下面以 Cisco Secure ACS 为例，介绍 RADIUS 服务器的配置过程。

❶ 在浏览器地址栏中输入“http://ACS-server-ip:2002”，访问 ACS 服务器，打开页面后依次选择 System Configuration→ACS Certificate Setup→Install ACS Certificate 命令，输入刚才申请的 Sadness 证书，并单击 Submit 按钮，如图 7-8 所示。

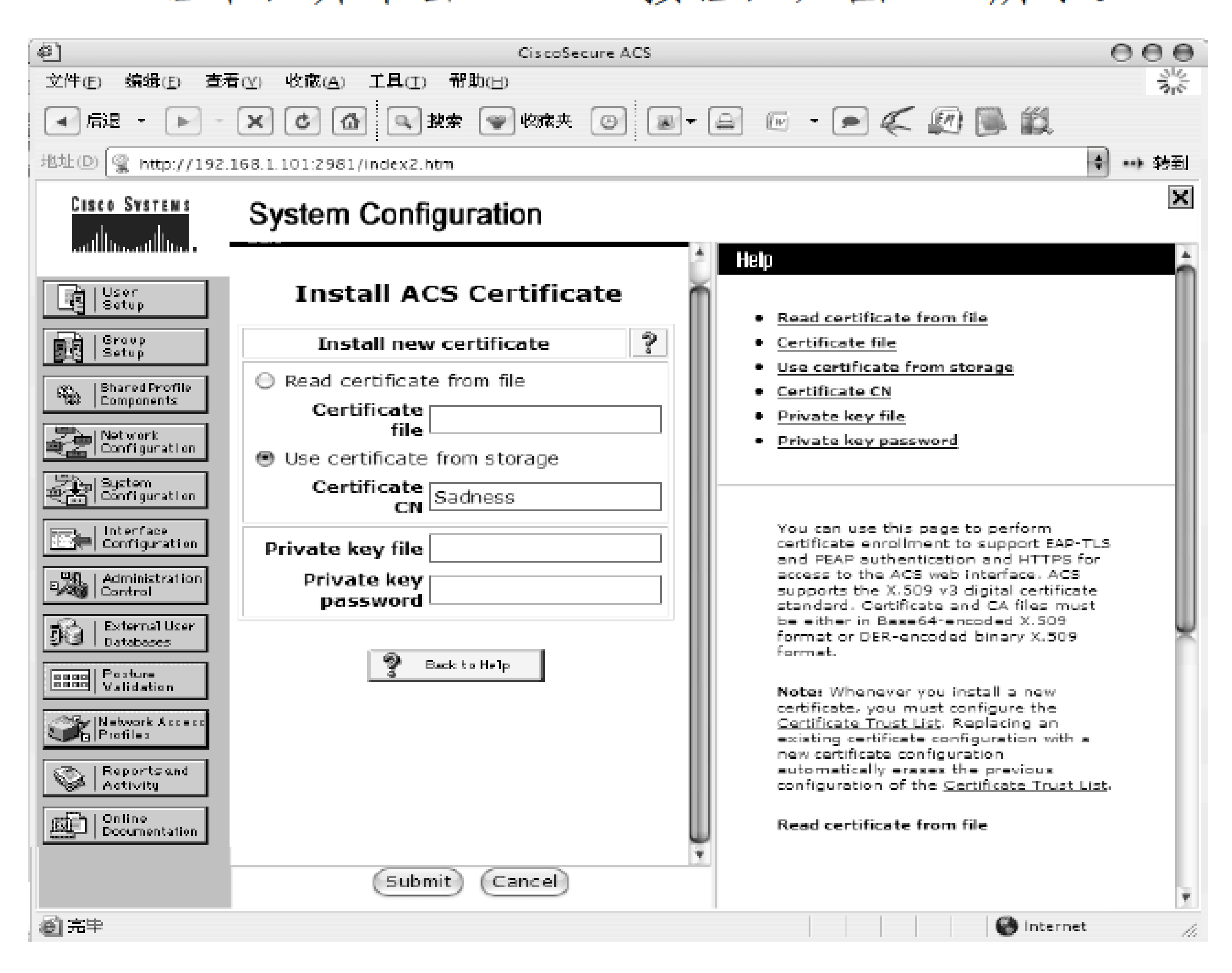


图 7-8　在 ACS 中应用证书

❷ 依次选择 System Configuration→ACS Certificate Setup→Install ACS Certificate→Edit Certificate Trust List 命令，选择 AD Server 上的根证书作为信任证书，然后单击 Submit 按钮，如图 7-9 所示。

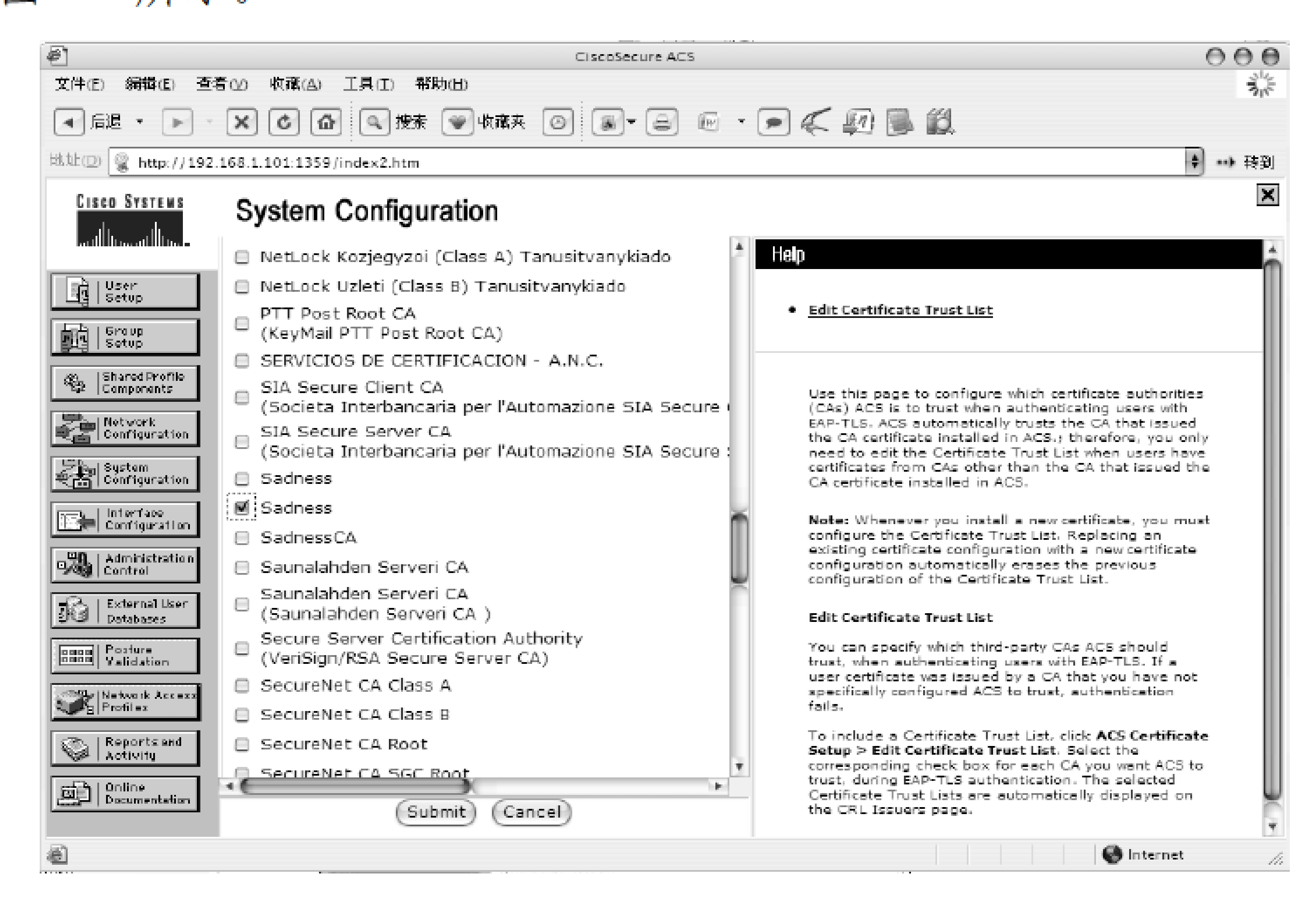


图 7-9　在 ACS 中添加根证书

❸ 依次选择 System Configuration→Global Authentication Setup 命令，选中 Allow EAP-MSCHAP v2 及 Allow EAP-GTC 两个复选框，并单击 Submit 按钮，如图 7-10 所示。

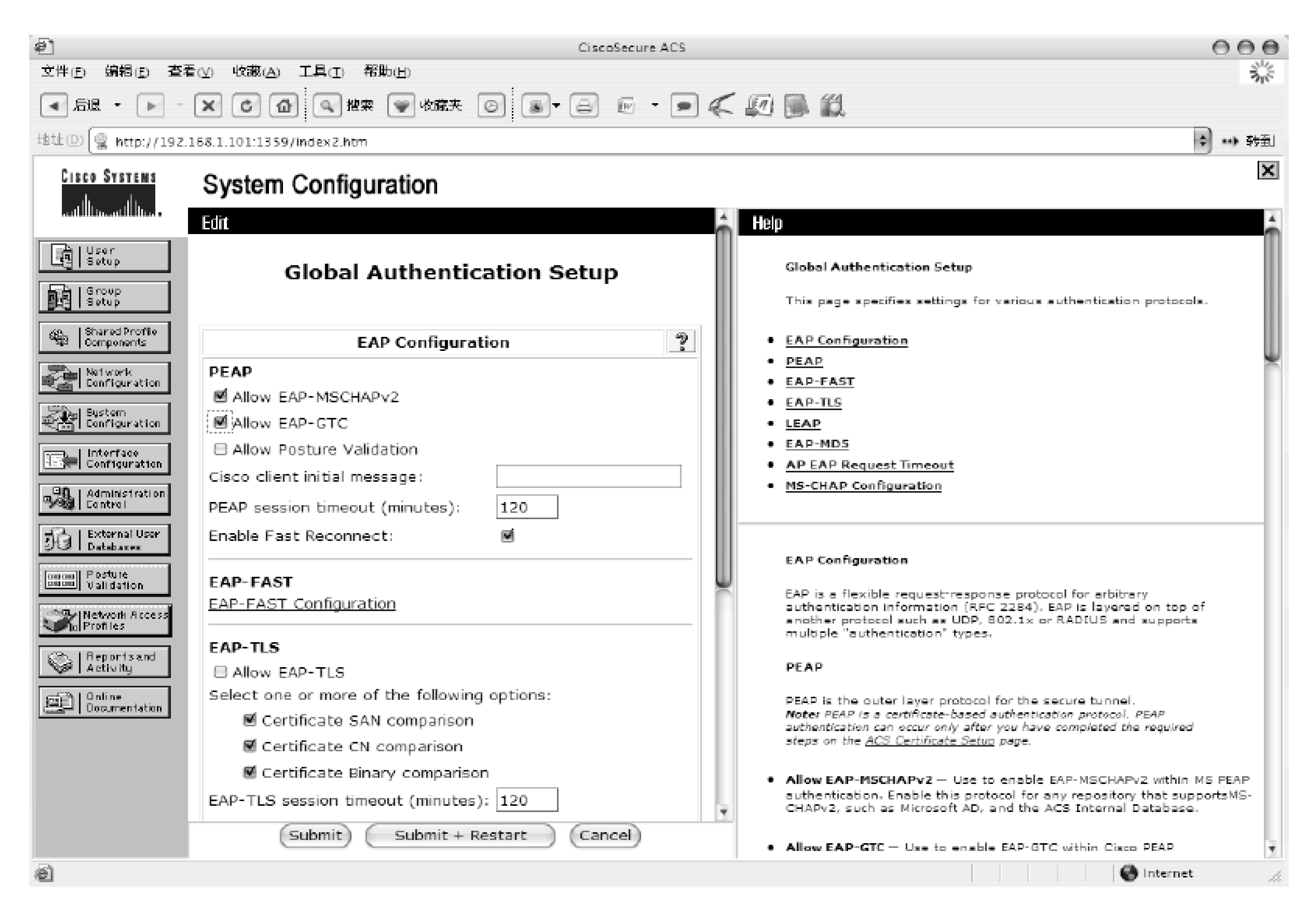


图 7-10　在 ACS 中配置全局认证属性

❹ 依次选择 External User Databases→Database Configuration→Windows Database→Configure 命令。在 Configure Domain List 下，将 Available Dornains 列表框中所在的域名称移动到 Domain List 列表框中，如图 7-11 所示。

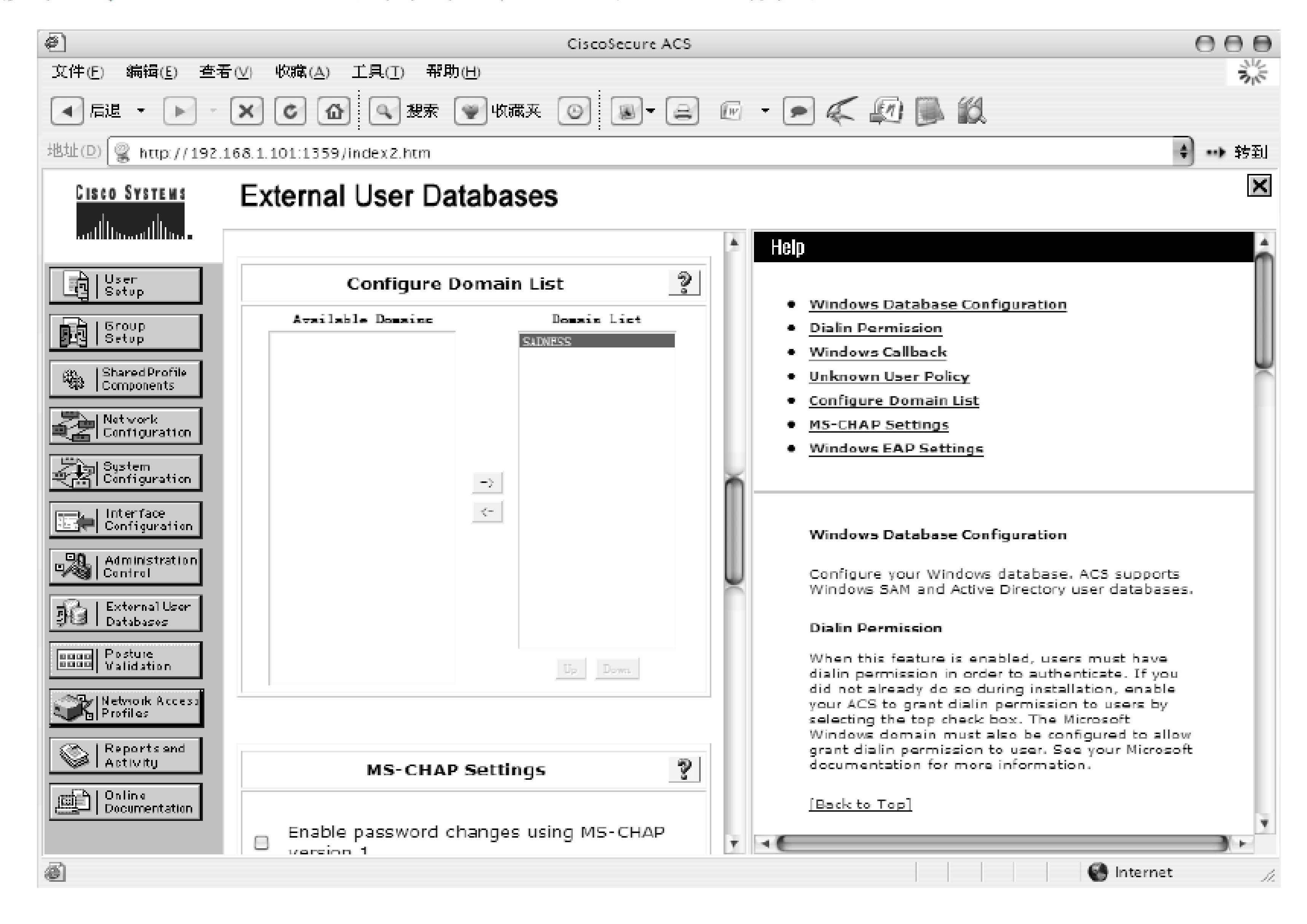


图 7-11　配置域列表

❺ 在 Windows EAP Settings 的 Machine Authentication 下，选中 Enable PEAP machine authentication 和 Enable EAP-TLS machine authentication 两个复选框，如图 7-12 所示。

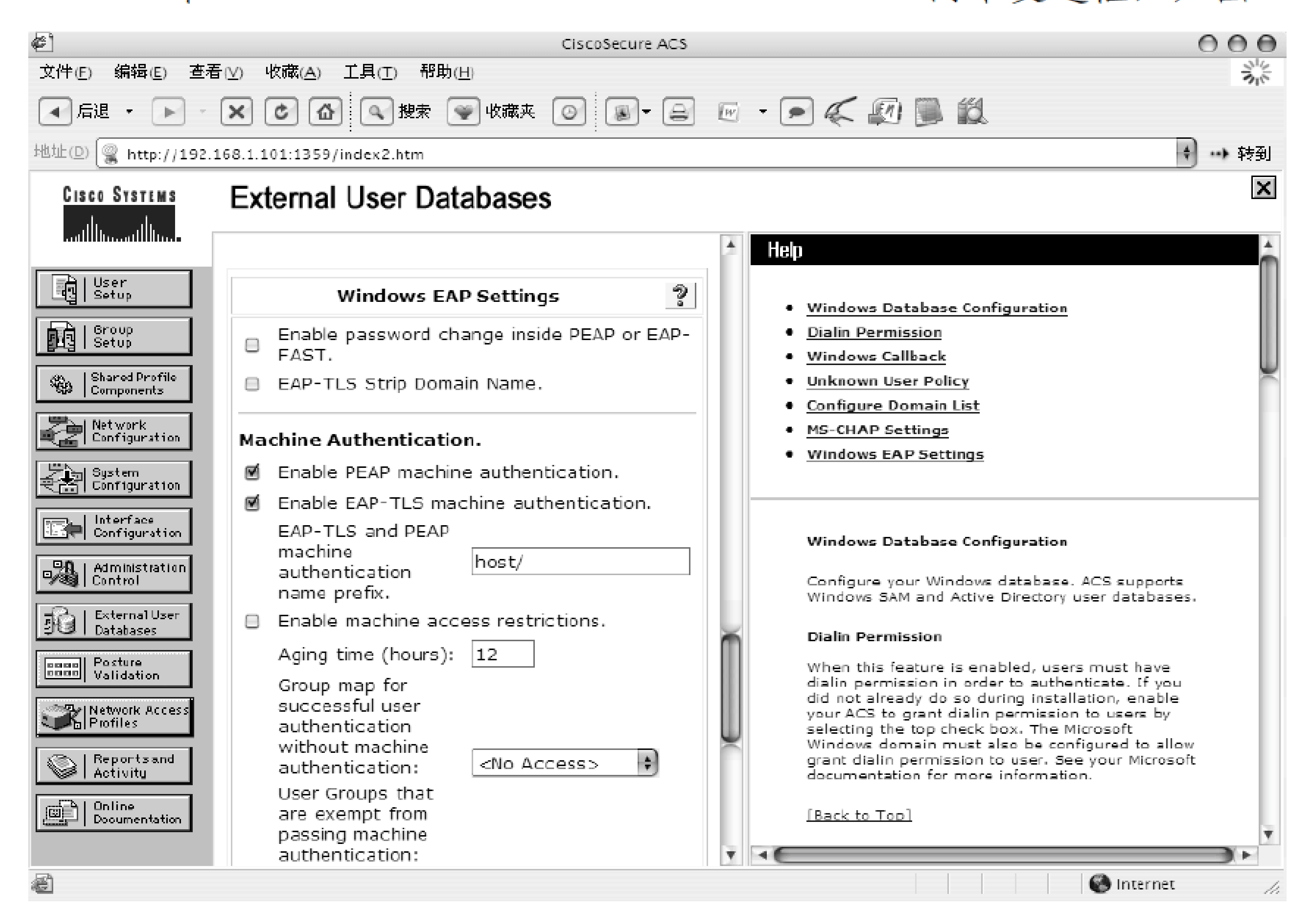


图 7-12　配置 Windows EAP

❻ 依次选择 External User Databases→Unknown User Policy→Check the following external user databases 命令，将 External Databases 列表框中的 Windows Database 移动到右边的 Selected Databases 列表框中，完成后再重启服务，如图 7-13 所示。

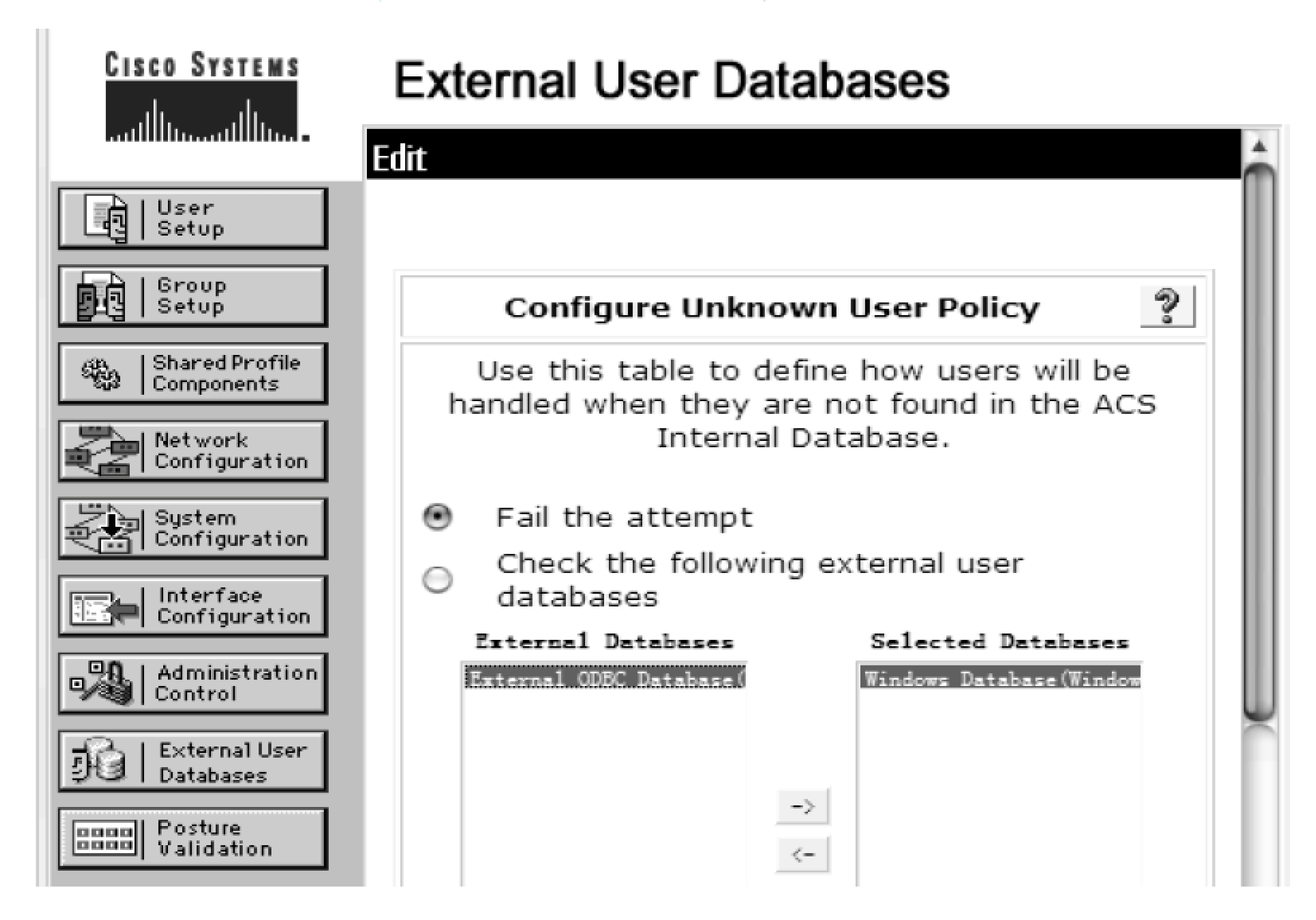


图 7-13　选择外部用户数据库

❼ 由于使用 AD 的用户名作为认证和授权，因此须将此 ACS 中的 Group 与 AD 的 Group 映射。依次选择 External User Database→Database Group Mappings→Windows Database→New Configure 命令，在 Detected Domains 列表框中选择 SADNESS，并单击 Submit 按钮，如图 7-14 所示。

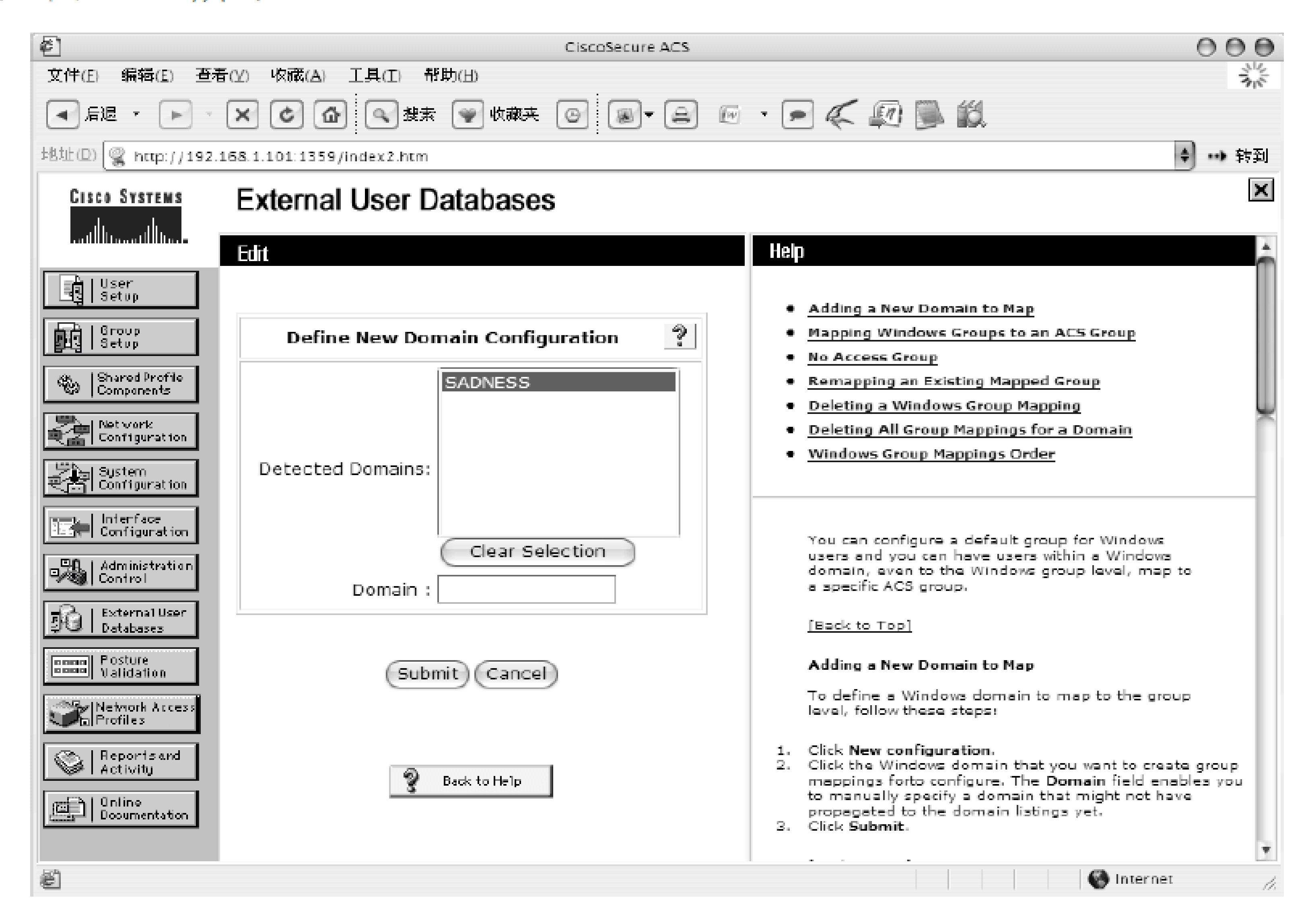


图 7-14 选择域

❽ 单击 SADNESS 链接，在打开的新页面中，从列表框中选择 Add Mapping 一项，并把 NT Groups 列表框中的组添加到 Selected 列表框中，同时在 Cisco Secure group 下拉列表框中选择 ACS 的组，并单击 Submit 按钮，如图 7-15 所示。

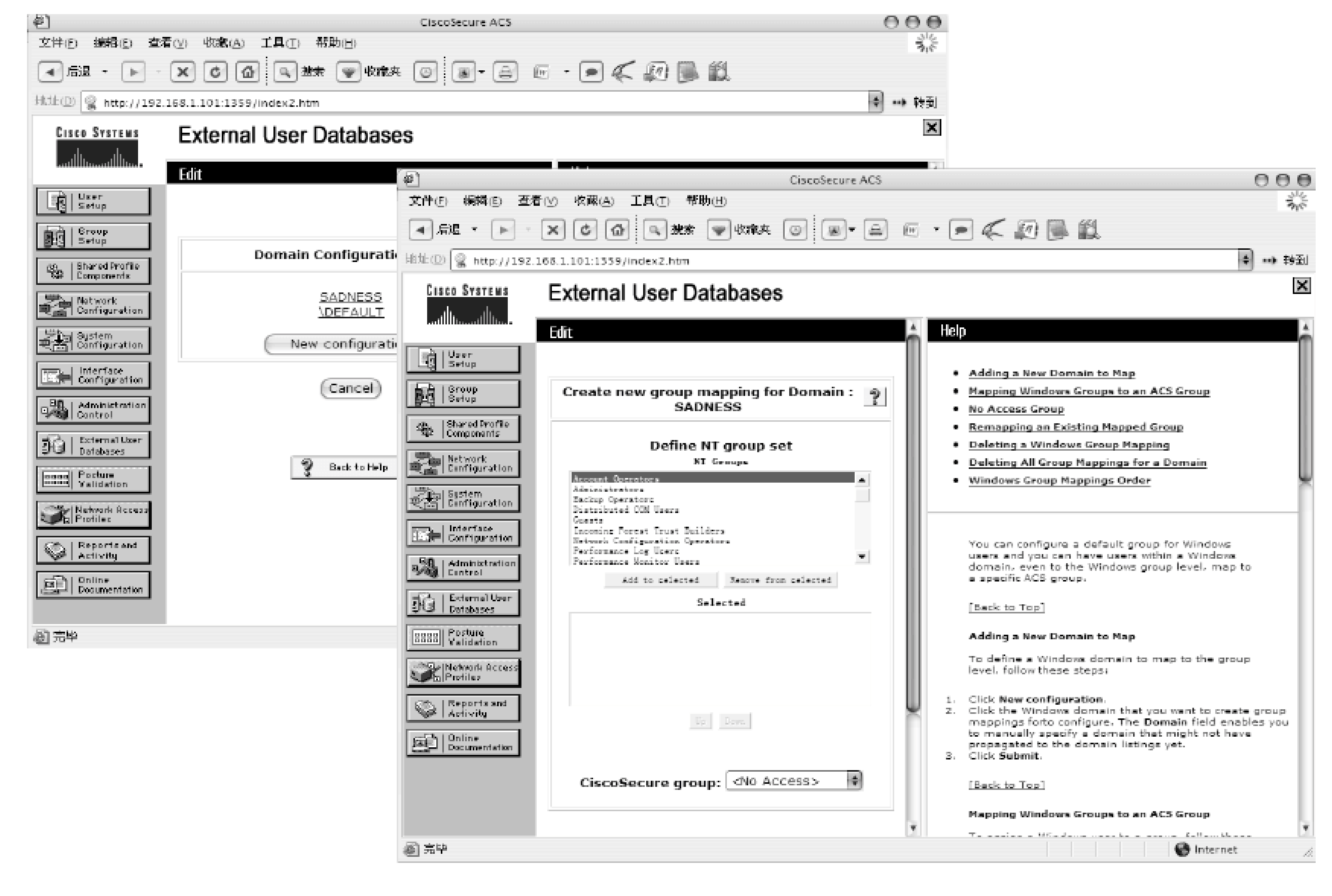


图 7-15 选择要映射的 Group

❾ 在 802.1x 认证中，所有使用 802.1x 交换机都是 RADIUS 服务器的一个客户端，因此需要向 RADIUS 服务器中添加一个客户端，添加方法请参见 6.3.3 一节。这里需要在主机名和 IP 地址文本框中，分别填入需要使用 802.1x 交换机的名称和 IP，认证类型选择 RADIUS(IETF)，如图 7-16 所示。

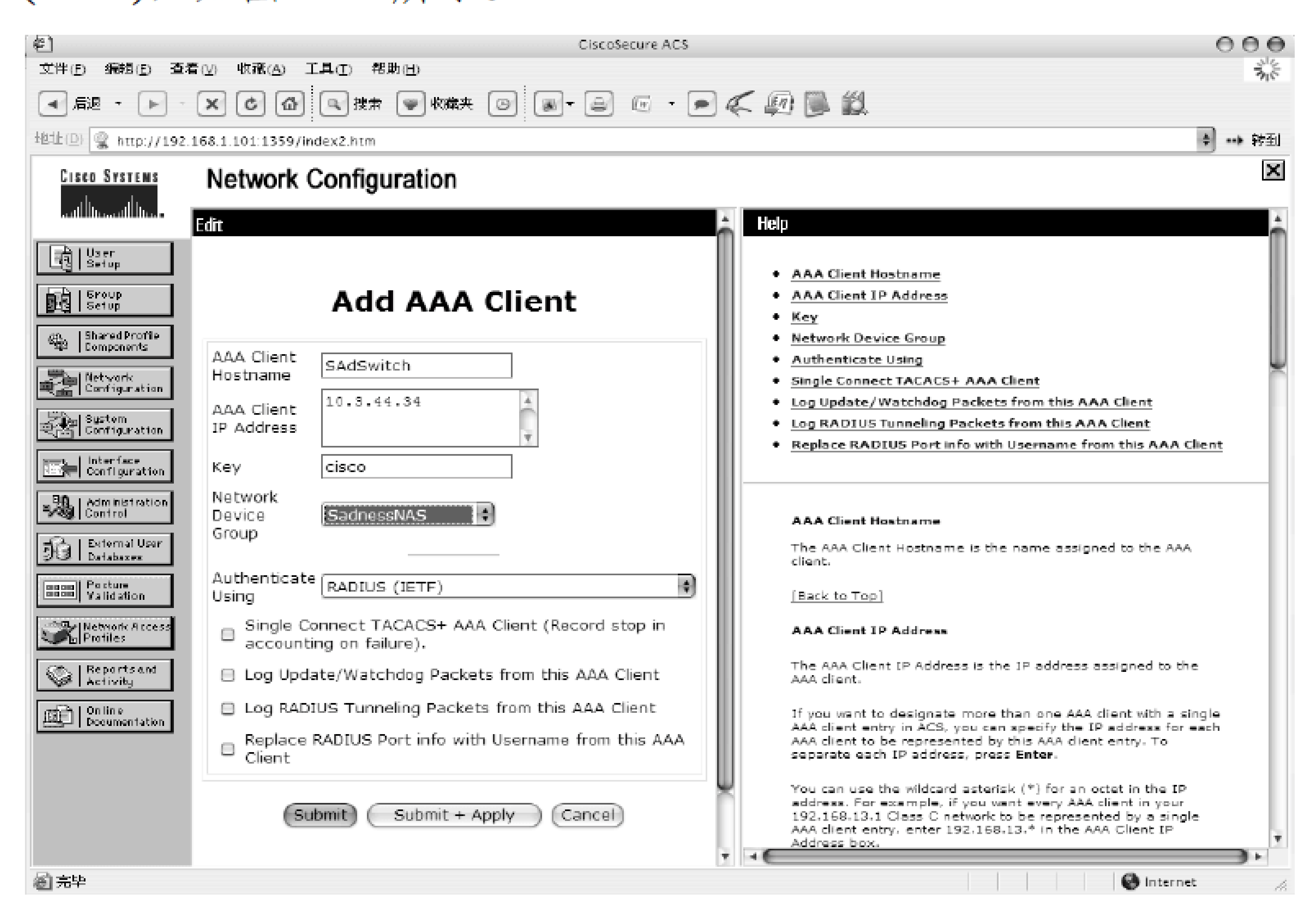


图 7-16　添加 AAA 客户端

3. 在网络接入设备(交换机、AP)上启用 802.1x 认证

1)　在 Cisco 交换机上启用 802.1x 认证

对使用以太网接入用户实施 802.1x 认证时，需要在交换机上配置使用 802.1x 认证。例如，希望用户认证成功则进入用户 VLAN(VLAN100)，如果认证失败，则进入 VLAN 200。其配置过程如下。

❶ 在全局配置模式下启用 AAA。

```
Switch(config)#aaa newmodel
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network default group radius
```

❷ 配置 RADIUS 服务器或服务器组。

```
Switch(config)# radius-server host 192.168.1.101 key Cisco
Switch(config)#radius-server vsa send authentication
```

❸ 在全局模式下启用 802.1x 认证。

```
Switch(config)#dot1x systemauthcontrol
Switch(config)#dot1x guestvlan supplicant
```

❹ 将需要实施用户接入控制的端口配置为 802.1x。

```
Switch(config)#Interface  fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x guestvlan 100
```

```
Switch(config-if)#dot1x authfail vlan 200
Switch(config-if)#dot1x hostmode multihost
```

2) 在 AP 上启用 802.1x 认证

对使用无线局域网接入用户实施 802.1x 认证时，需要在 AP 上配置使用 802.1x 认证。假设，Sadness 公司使用 Cisco Aironet 系列无线 AP，其配置过程如下。

❶ 通过 Web 浏览器或配置程序，打开 AP 配置界面。在 AP 上定义不同的 VLAN，用于不同类型的用户接入，如图 7-17 所示。

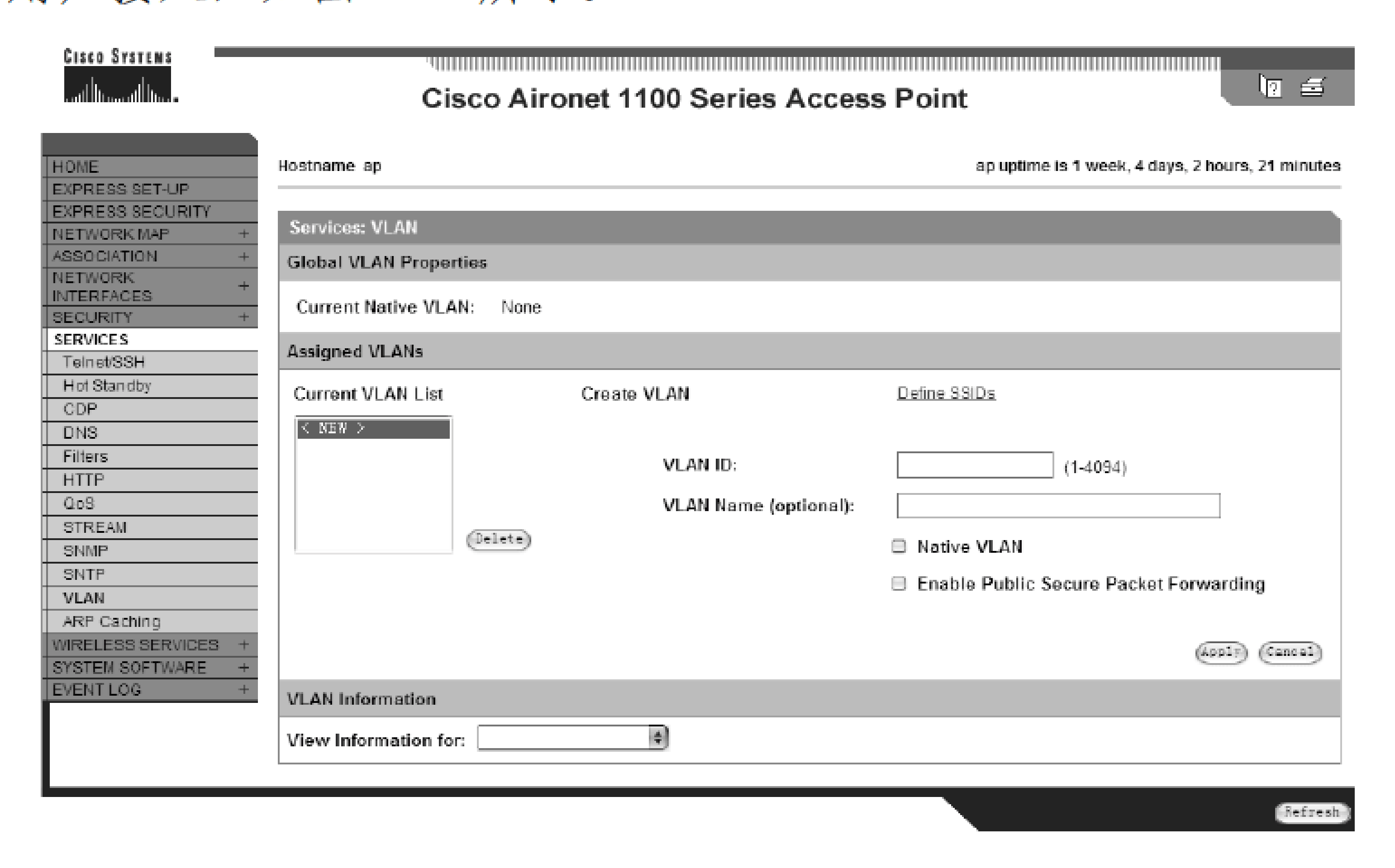


图 7-17　在 AP 上配置 VLAN

❷ 为不同的 VLAN 分配不同的 SSID，并且可以配置客户所使用的认证类型，如图 7-18 所示。

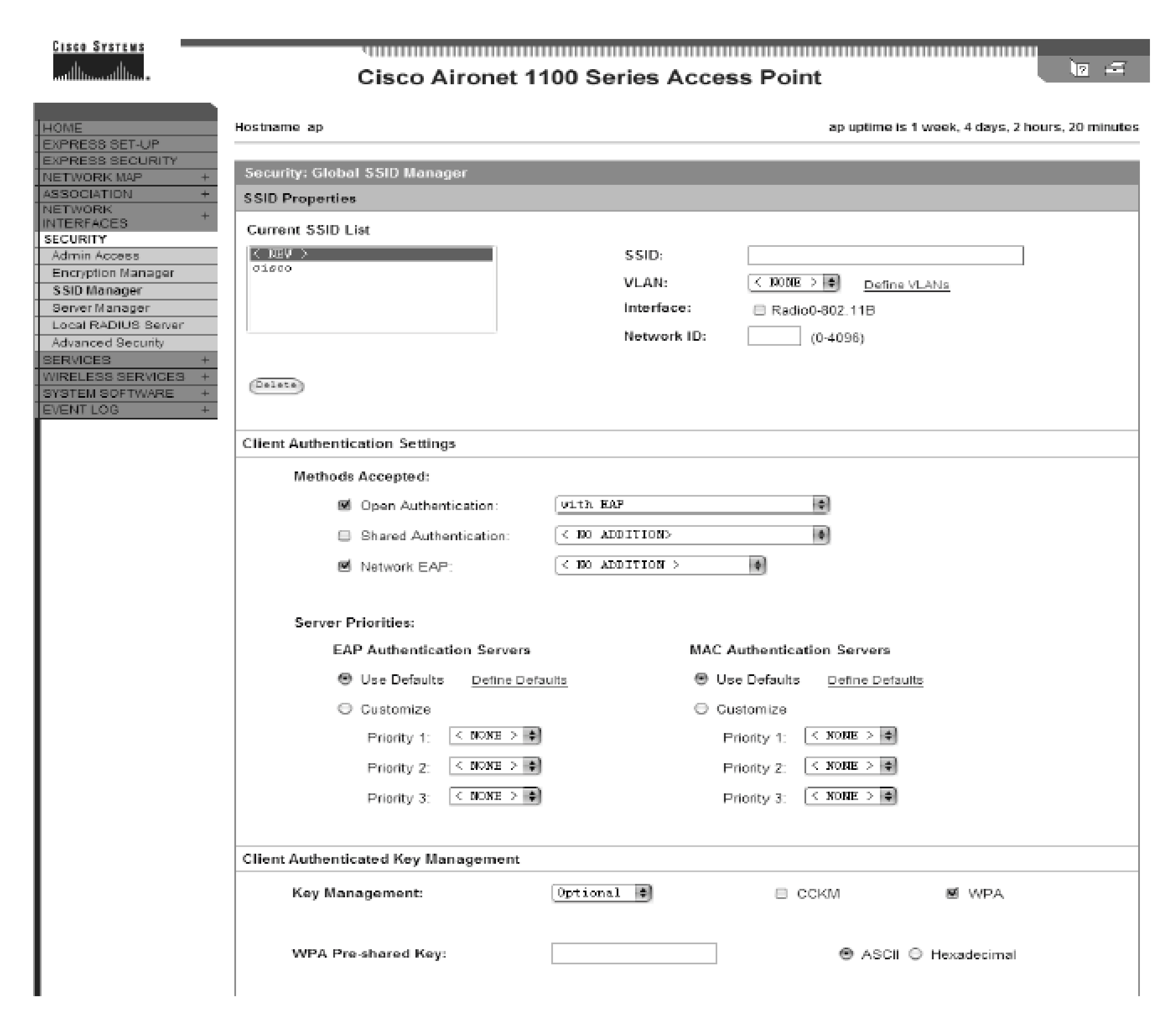


图 7-18　配置 SSID

❸ Cisco Aironet 系列无线 AP 支持本地 RADIUS 服务器。若没有本地 RADIUS 服务器，可在 AP 上配置相应的 RADIUS 服务器，如图 7-19 所示。

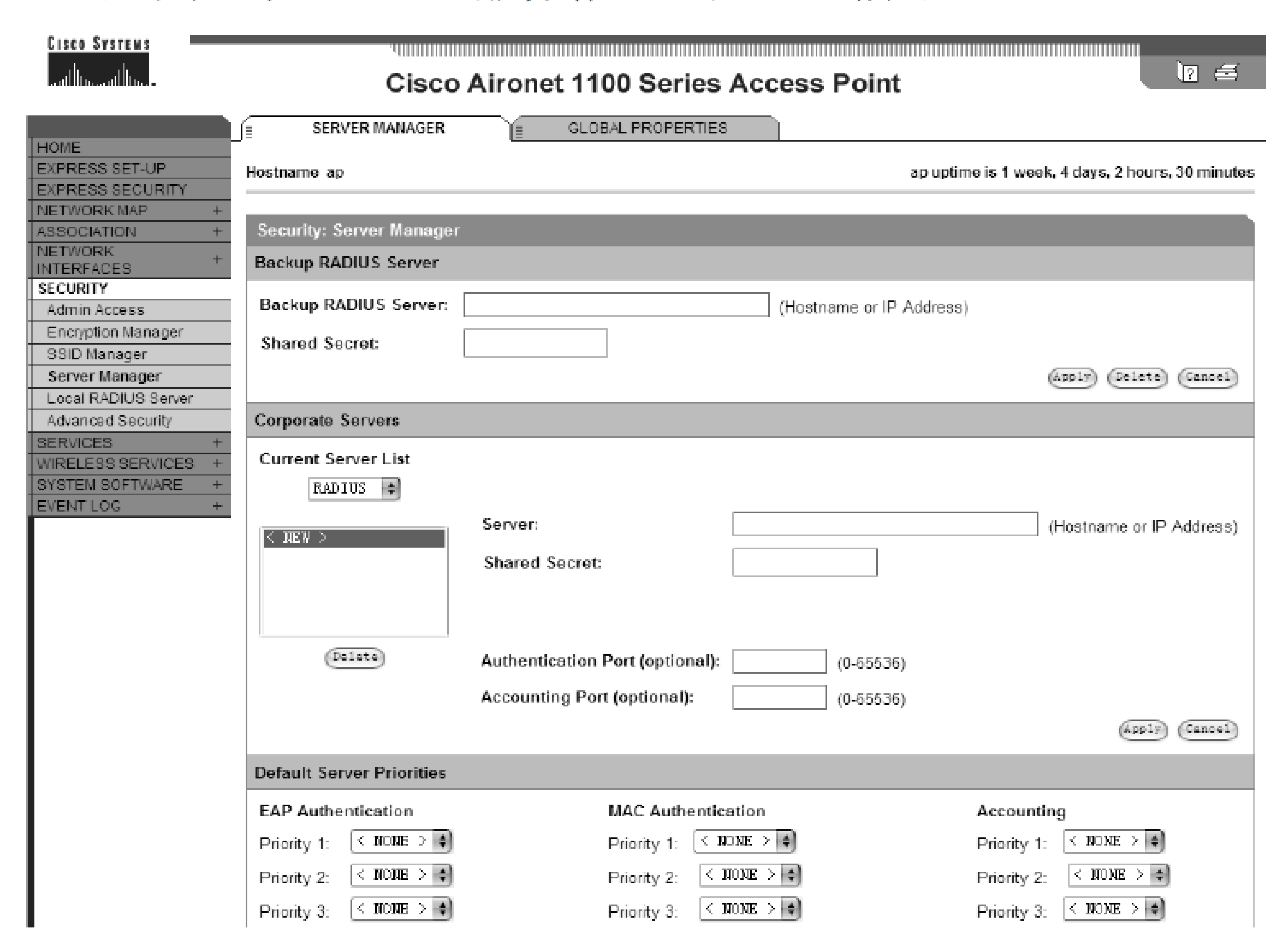


图 7-19　配置 RADIUS 服务器

❹ 为了无线网络安全，Cisco AP 还支持基于 WEP(Wired Equivalent Privacy，有线对等保密)协议来设置专门的安全机制，进行业务流的加密和结点的认证，其配置方法如图 7-20 所示。WEP 主要用于无线局域网中链路层信息数据的保密，它采用对称加密机理，即数据的加密和解密采用相同的密钥和加密算法。

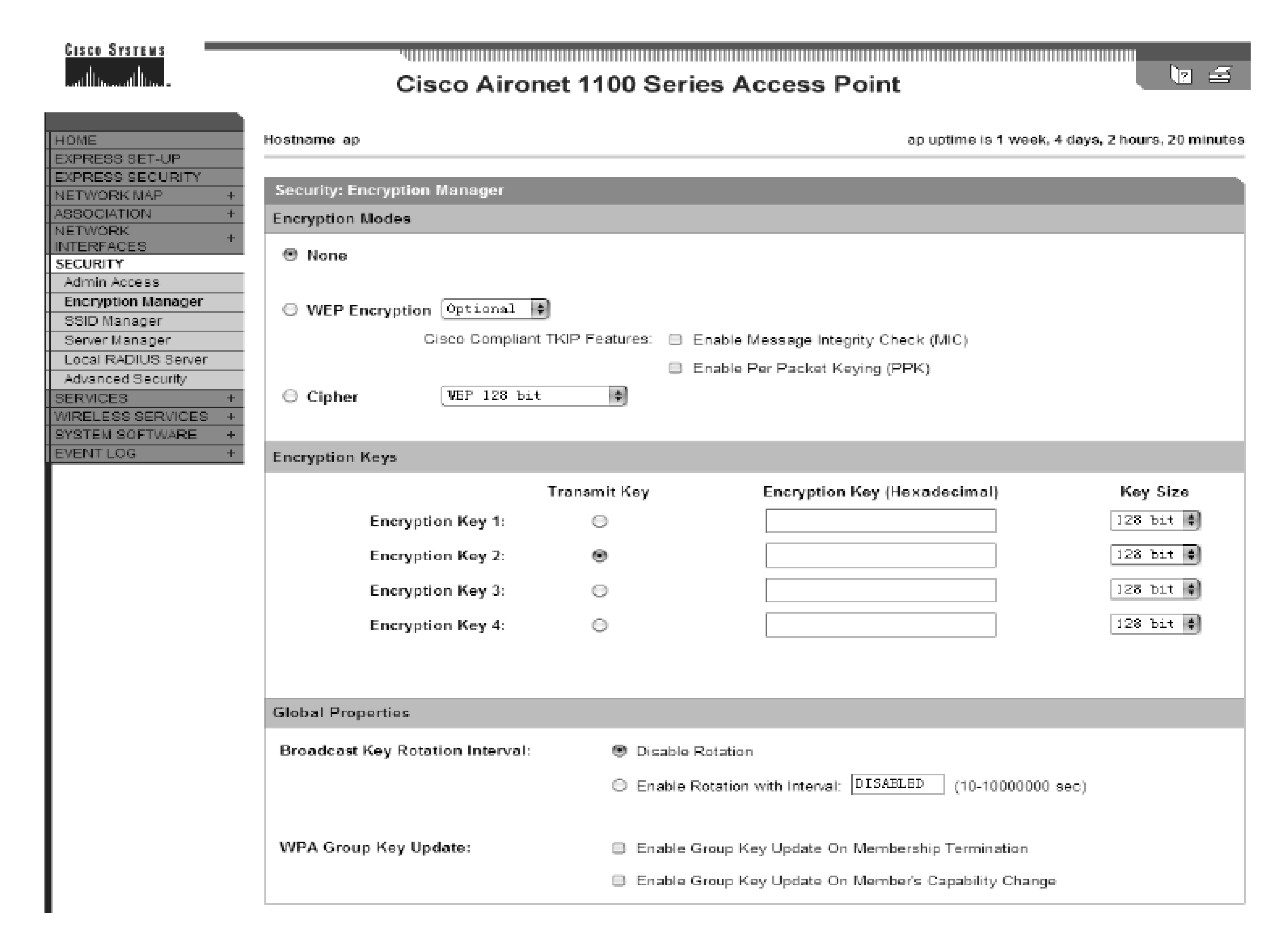


图 7-20　配置 WEP 加密

4. 配置基于动态 VLAN 的 802.1x 认证

上面对交换机和 AP 进行 802.1x 认证配置时，都使用静态 VLAN。基于 Cisco ACS 和 Active Directory 的架构还支持动态 VLAN 的配置，即根据在 RADIUS 服务器上所定义的用户信息给用户分配特定的 VLAN，从而达到相对安全且相对灵活的网络结构。

配置基于动态 VLAN 的 802.1x 认证主要包括两部分，一部分是对 ACS 服务器进行配置；另一部分是对接入交换机的进行配置，下面分别给予介绍。

1) 配置 ACS 服务器

❶ 在浏览器地址栏中输入http://ACS-server-ip:2002，访问 ACS 服务器。打开页面后依次选择 Interface Configuration → RADIUS (IETF) 命令，选中 Tunnel-Type、Tunnel-Medium-Type 和 Tunnel-Private-Group-ID 三个复选框，如图 7-21 所示。

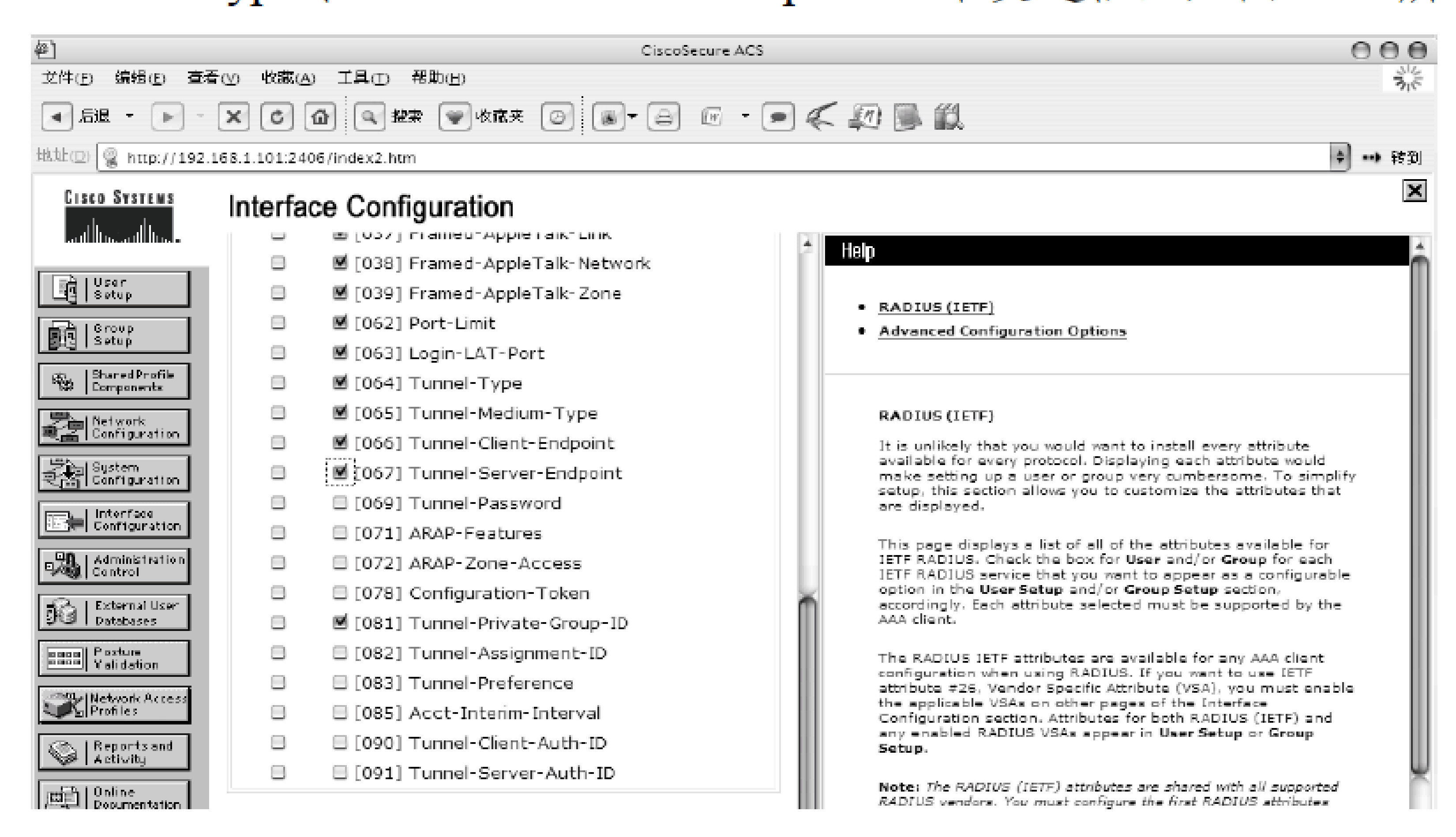


图 7-21 配置 RADIUS 属性

❷ 依次选择 Group Setup → Group:X → Edit Settings 命令，选中 Tunnel-Type、Tunnel-Medium-Type 和 Tunnel-Private-Group-ID 三个复选框，并将 Tunnel-Type 设为 VLAN，将 Tunnel-Medium-Type 设为 802，将 Tunnel-Private-Group-ID 设为此 Group 用户所要访问的 VLAN 号，如图 7-22 所示。

2) 配置接入交换机

采用基于动态 VLAN 的 802.1x 认证时，交换机上仅需进行如下配置。

❶ 在全局配置模式下启用 AAA。

```
Switch(config)#aaa newmodel
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network default group radius
```

❷ 配置 RADIUS 服务器或服务器组。

```
Switch(config)# radius-server host 192.168.1.101 key Cisco
Switch(config)#radius-server vsa send authentication
```

❸ 在全局模式下启用 802.1x 认证。

```
Switch(config)#dot1x systemauthcontrol
```

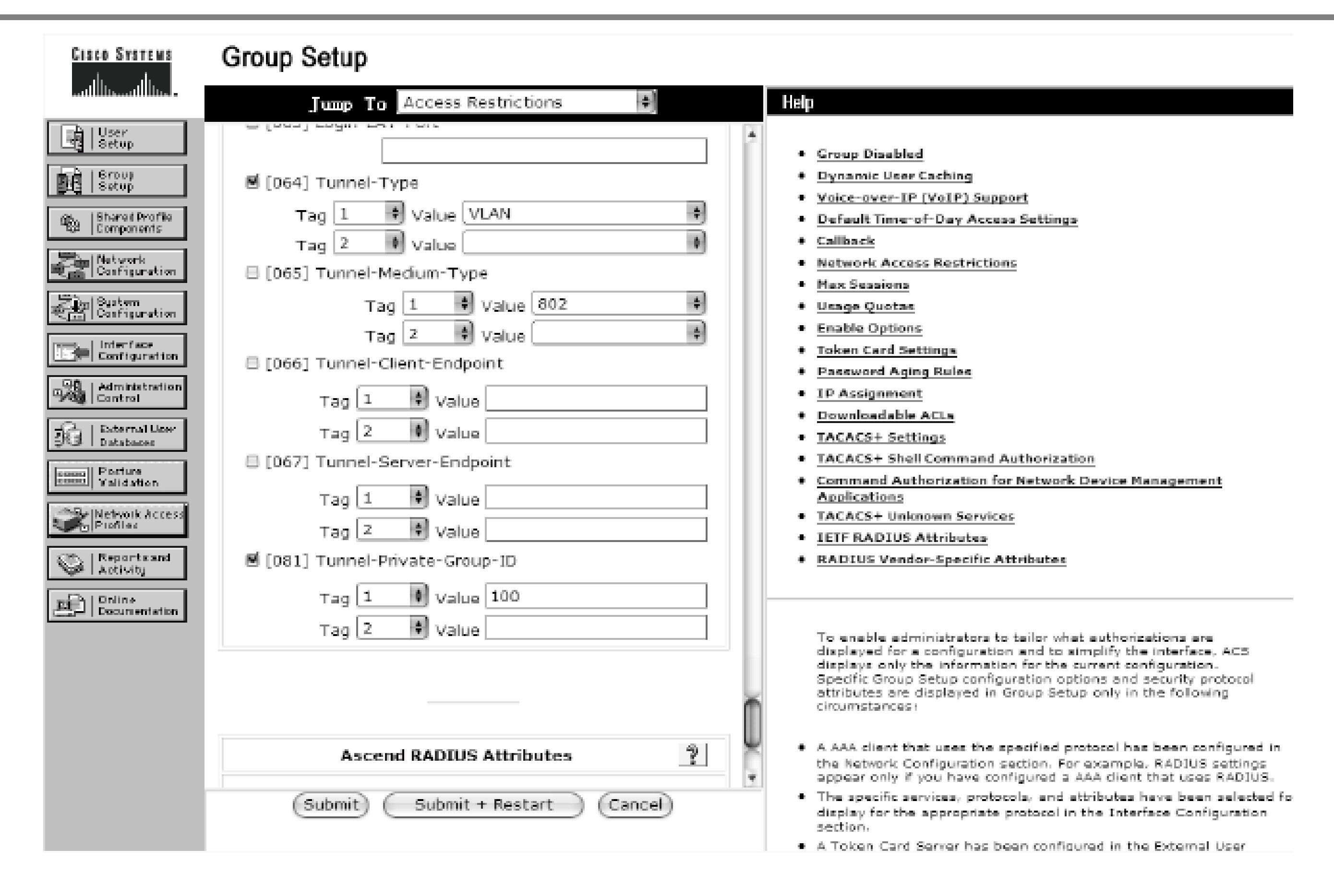


图 7-22　配置动态 VLAN

❹ 将需要实施基于动态 VLAN 的认证用户接入控制端口配置为 802.1x。

```
Switch(config)#Interface  fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
```

5. 配置 802.1x 客户端

802.1x 客户端可以是通过以太网接入的用户，也可以是以无线局域网接入的用户，它们的配置方法相似。下面以后者为例，介绍 802.1x 客户端的配置过程。

❶ 在浏览器中输入“http://CA-server-ip/certsrv”，在证书服务 Web 页面中单击【下载一个 CA 证书，证书链或 CRL】链接。在打开的【下载 CA 证书、证书链或 CRL】 Web 页面中单击【下载 CA 证书】链接，如图 7-23 所示。

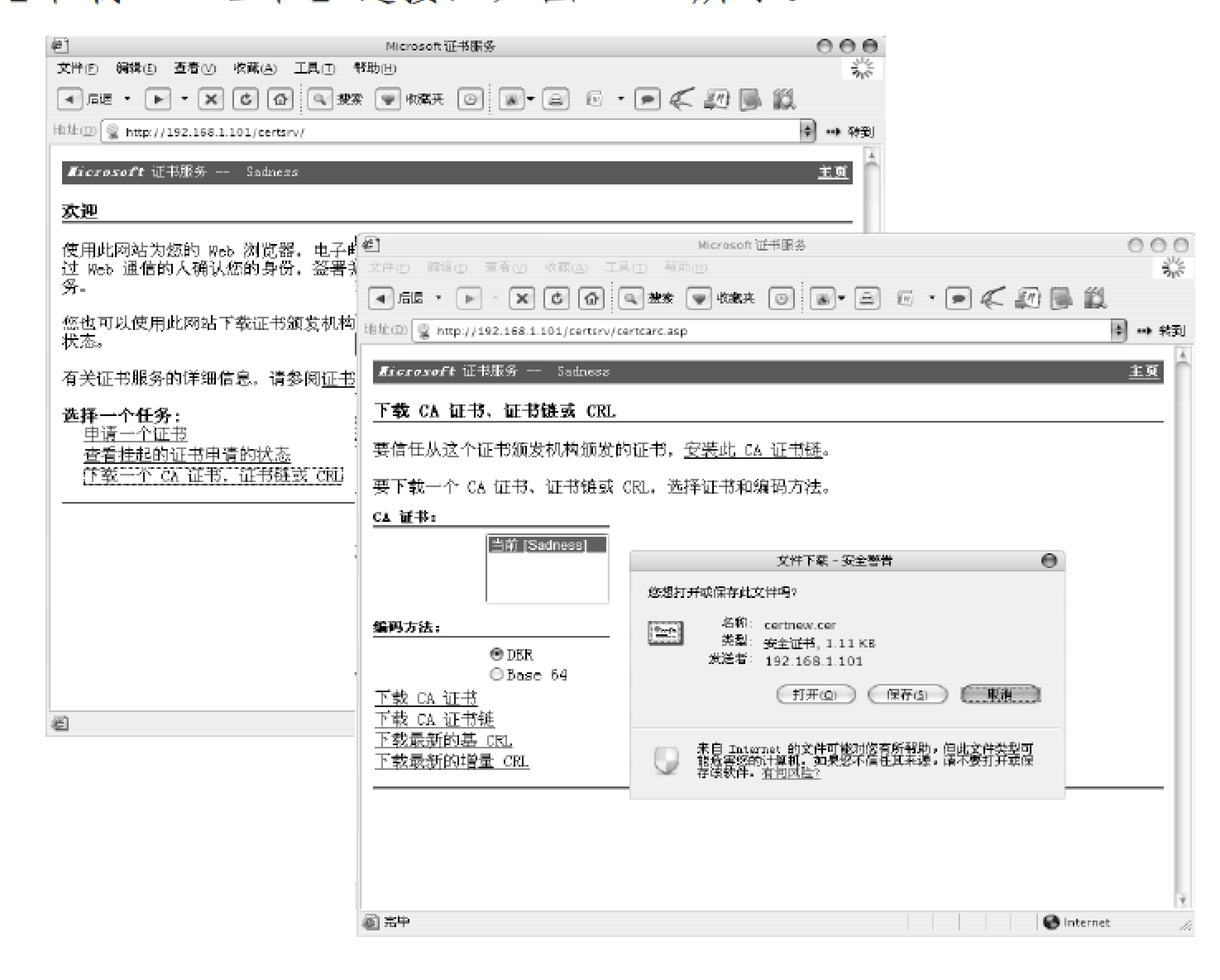


图 7-23　下载 CA 证书

❷ 双击已经下载的证书文件，在弹出的对话框中单击【安装证书】按钮，然后根据证书导入向导将证书保存到【受信任的根证书颁发机构】下的 Local Computer 中，然后单击【确定】按钮，如图 7-24 所示。



图 7-24　保存证书

❸ 打开【无线网络属性】对话框，选择【验证】选项卡，选中【启用此网络的 IEEE 802.1x 验证】复选框，并将【EAP 类型】下拉列表框设置为【受保护的 EAP(PEAP)】，选中【当计算机信息可用时验证为计算机】复选框，然后再单击【属性】按钮。在打开的【受保护的 EAP 属性】对话框中，选中【验证服务器证书】复选框，同时在【受信任的根证书颁发机构】列表框中选择相应的根证书颁发机构，这里选中 Sadness，并将【选择验证方法】下拉列表框设置为【安全密码(EAP-MSCHAP v2)】。最后单击【确认】按钮，如图 7-25 所示。这时将弹出提示框，询问是否自动使用 Windows 登录名和密码。



图 7-25　配置 802.1x

❹ 当连入网络时，如果在前面一步没有选中【自动使用 Windows 登录名和密码】复选框，则会在右下角会弹出一个提示信息，如图 7-26 所示。

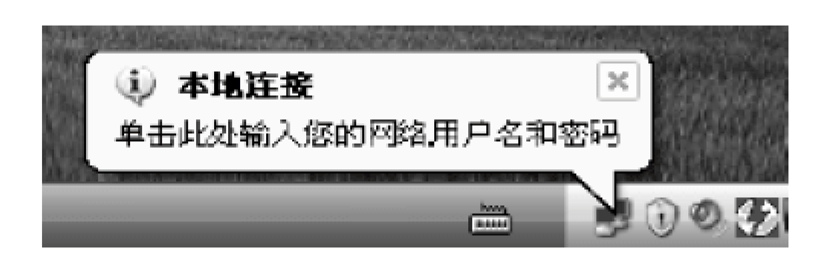


图 7-26　提示需输入网络用户名和密码

❺ 单击右下角的提示信息后，输入正确的用户名和密码，即可连入网络，如图 7-27 所示。



图 7-27　输入网络用户名和密码

点评与拓展：802.1x 为传统网络提供了一个简单的接入身份认证功能，应用实例介绍了基于 Windows AD 账号的统一身份认证接入配置的方法；在提高网络安全的同时，统一的账号也带来了很大的舒适性，并且可以用于基于无线接入技术的共享型网络。802.1x 虽然解决了网络接入身份认证的问题，但却无法阻止一些中毒的主机接入网络，而中毒的原因通常是软件更新不及时所致。因此在后面两节中，我们将介绍微软的 WSUS 自动升级服务以及 Cisco 的网络接入控制(Cisco NAC)架构。

7.2　Windows 自动更新

应用实例导航:架设 Windows 系统补丁服务器

※场景呈现

ABC 学院接入到中国教育科研网的带宽是 100M，随着用户的添加，用户普遍反映网速太慢。网络管理员在监测网络流量时发现，很大一部分流量是用户的 Windows 系统更新。为此，该学院的网络中心决定安装一台 WSUS 服务器，为学院内部用户提供 Windows 系统

更新服务以减少这方面的网络流量，同时还能提高内部用户 Windows 系统更新的速度。

假设拟安装 WSUS 的服务器 IP 地址是 222.190.68.17，域名是 wsus.abc.edu.cn。

※技术要领

(1) 安装 WSUS 3.0 服务器端软件；
(2) 配置 WSUS 服务器；
(3) 管理 WSUS 服务器；
(4) 配置 WSUS 客户端，使其从 WSUS 服务器获取 Windows 系统更新。

7.2.1 WSUS 简介

微软经常会发布其产品补丁程序，如果没有及时安装这些补丁，计算机将会有漏洞暴露在互联网上。所以即使有病毒防火墙的保护，一旦相应的病毒或攻击发作，机器仍然会很容易中招，而且还会成为别人进攻的对象。

Windows Server Update Services(简称 WSUS)，是微软公司提供的一种免费软件，它提供了 Windows 部分操作系统的关键更新的分发。网络中心基于此技术在岛内构建了一个 WSUS 服务器，向全岛的网络用户提供免费的 WSUS 服务，使用此服务可以快速进行部分 Windows 操作系统的关键补丁的更新，减轻在病毒发作时从美国微软更新的时间，同时通过运行如下所附的设置程序将会将用户的计算机的更新完全调节好，从而免除用户担心更新问题的烦恼。

WSUS 目前提供对微软 15 个新产品和 8 个新分类的更新，新产品涵盖了 Windows 2000 家族、Windows XP 家族、Windows 2003 家族、Office 2000/XP/2003 家族、SQL Server 等；提供更新的 8 个分类为：Feature Pack、Service Pack、安全更新程序、更新程序、更新程序集、工具、关键更新程序、驱动程序。当适用于用户的计算机的重要更新发布时，它会及时提醒用户下载和安装。使用自动更新可以在第一时间更新操作系统以及其他微软产品，修复系统及程序的漏洞，保护计算机安全。使用此更新同微软的在线升级并无冲突，此更新系统可同步微软网站,更新的一半以上都是一些关键更新，为使补丁齐全，用户仍然可以随时访问 http://windowsupdate.microsoft.com/进行在线升级打全补丁。

WSUS 服务器和 Microsoft Update 实现客户端计算机自动更新的方式完全相同，通过 WSUS 可以实现更新程序的集中管理和分发，它的主要优点如下。

- ✧ 通过选择的方式将更新程序(包含 Feature Pack、Service Pack、安全更新、关键更新、更新程序、更新程序集、工具、驱动程序等，可选择)从 Microsoft Update 下载至本地安装源，节省企业外部网络带宽。
- ✧ 对更新程序进行管理，控制更新程序的分发；可以批准更新在客户端计算机上进行安装，或者仅仅是检测客户端计算机是否需要此更新程序，也可以拒绝此更新程序。
- ✧ 对网络中的客户端计算机进行分组，控制更新程序在不同客户端计算机上的分发。

因此，现在的微软更新服务体系为三级结构：Microsoft Update→本地企业网络中的

WSUS 服务器→客户端计算机的自动更新，如图 7-28 所示。

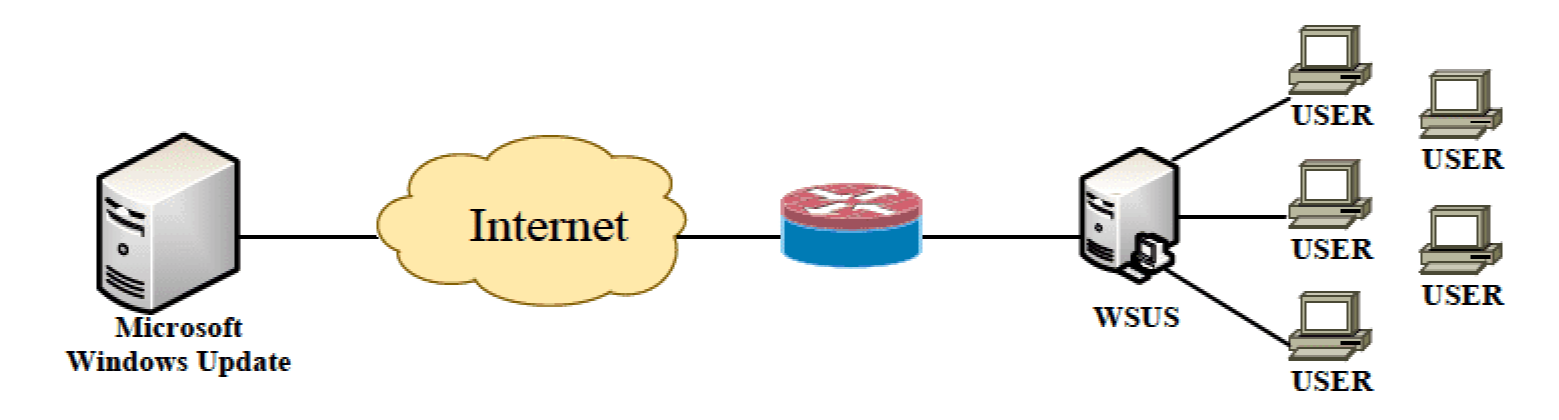


图 7-28　三级更新结构

在部署 WSUS 之后，只需要配置客户端计算机使用 WSUS 服务器上的更新服务，就可以轻松的享受 WSUS 服务器所带来的好处。例如，当大中型企业网络部署 WSUS 服务器以后，内部客户端计算机可自动访问 WSUS 服务器来获取更新，免除了频繁手动安装补丁的麻烦，节省了大量的外部网络带宽。

7.2.2　安装 WSUS 服务器

要安装 WSUS 3.0 服务器软件，文件系统必须满足以下要求。

✧ 系统分区和安装 WSUS 3.0 的分区都必须使用 NTFS 文件系统进行格式化。
✧ 系统分区至少留出 1 GB 的可用空间。
✧ WSUS 用于存储内容的卷至少留出 20 GB 的可用空间，但最好留出 30 GB 的可用空间。
✧ WSUS 安装程序安装 Windows Internal Database 的卷至少留出 2 GB 的可用空间。

在满足上述条件的服务器上，安装 WSUS 3.0 服务器的过程如下。

❶ 从微软网站下载如表 7-1 所示的软件或系统补丁。

表 7-1　安装 WSUS 3.0 需准备的文件

软件名称	下　载　地　址
Windows Server 2003 Service Pack 2	http://technet.microsoft.com/zh-cn/windowsserver/bb229701.aspx 文件名为：WindowsServer2003-KB914961-SP2-x86-CHS.exe
后台智能传送服务（BITS）2.0	http://go.microsoft.com/fwlink/?LinkID=47251 文件名为：WindowsServer2003-KB842773-x86-chs.exe
Microsoft.NET Framework 2.0 版可重分发软件包（x86）	http://go.microsoft.com/fwlink/?LinkID=68935 文件名为：dotnetfx.exe
Microsoft Report Viewer Redistributable 2005	http://go.microsoft.com/fwlink/?LinkID=70410 文件名为：ReportViewer.exe
WSUS 3.0 安装程序	http://technet.microsoft.com/en-us/wsus/bb466190 文件名为：WSUS3Setupx86.exe

❷ 安装 IIS。在安装过程中需要选中 ASP.NET 及【启用网络 COM+ 访问】复选框，如图 7-29 所示。

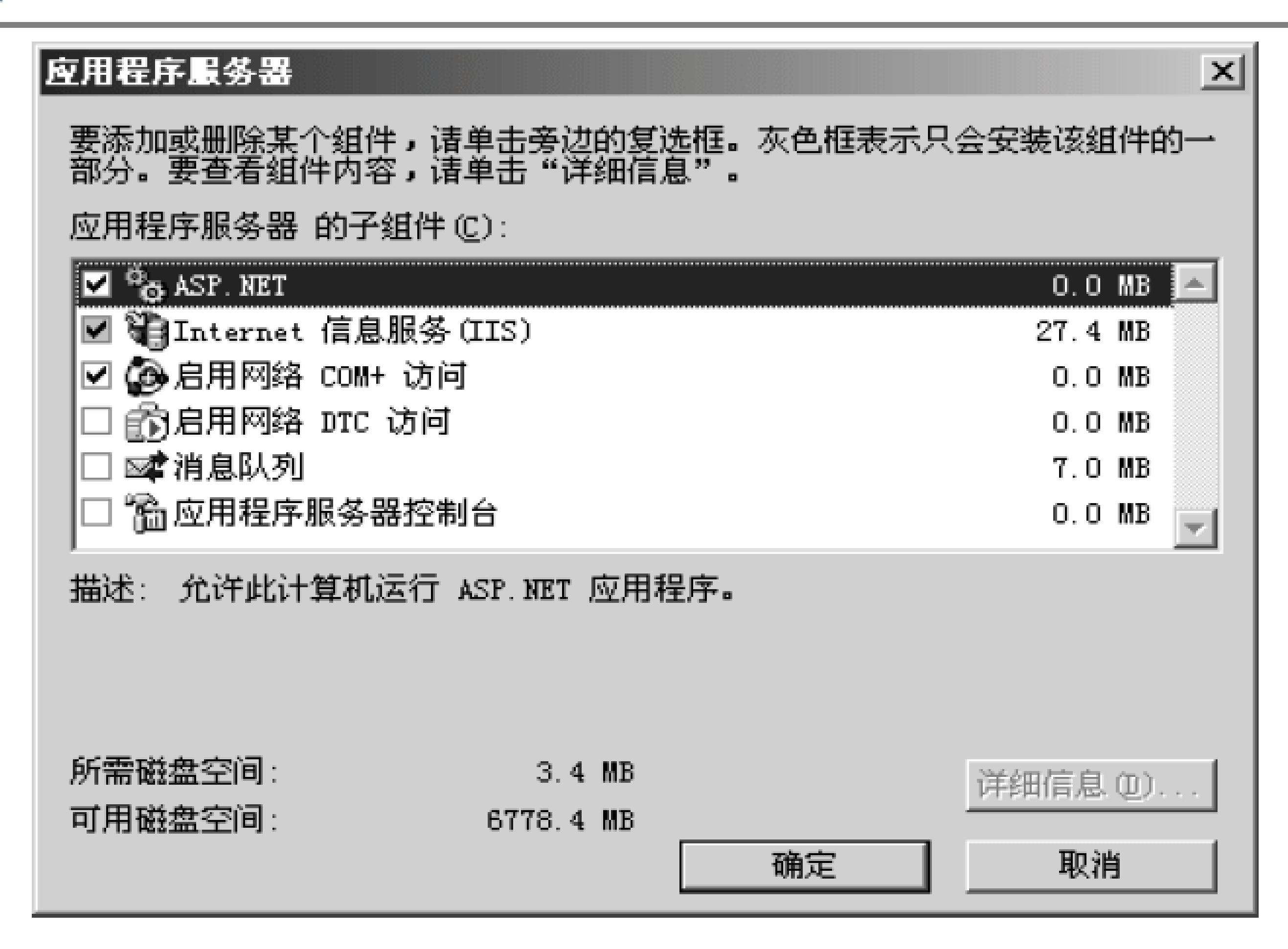


图 7-29　安装 IIS

❸ 安装 Windows Server 2003 Service Pack 2。

❹ 安装后台智能传送服务(BITS)2.0、Microsoft.NET Framework 2.0 版可重分发软件包和 Microsoft Report Viewer Redistributable 2005 等 WSUS 3.0 安装必备组件，这些组件都是安装 WSUS 3.0 的先决条件，安装方法很简单，这里就不做介绍了（注：如果只安装 Windows Server 2003 Service Pack 1，还需要安装用于 Windows Server 2003 的 Microsoft 管理控制台 3.0)。

❺ 双击 WSUS 服务器的安装程序 WSUSSetup.exe，打开安装向导页，然后单击【下一步】按钮继续，如图 7-30 所示。

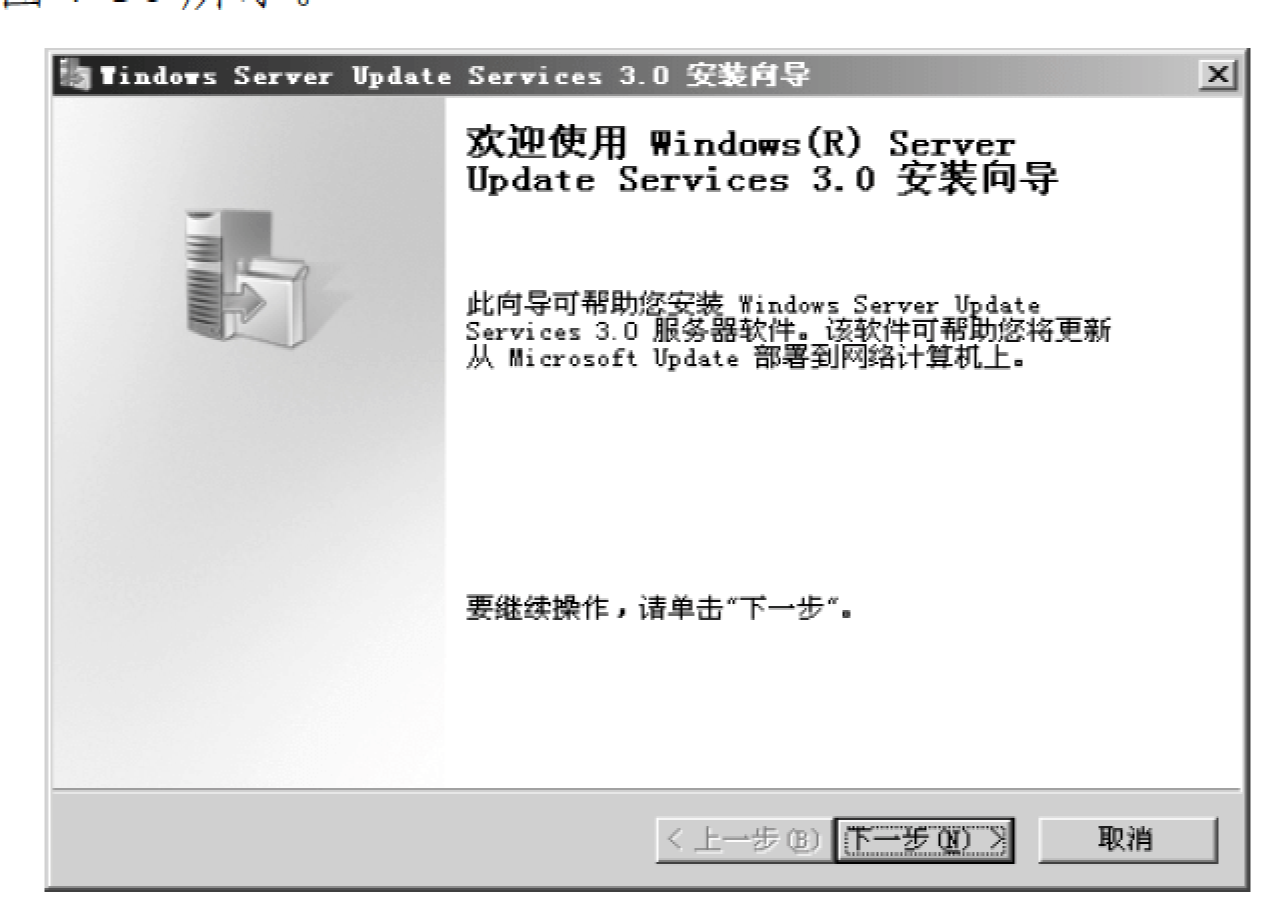


图 7-30　WSUS 安装向导

❻ 在【安装模式选择】向导页中，如果希望在此计算机上安装服务器，选中【包括管理控制台的完整服务器安装】单选按钮；如果仅希望安装管理控制台，选中【仅限管理控制台】 单选按钮。这里选择前者，如图 7-31 所示。



图 7-31　【安装模式选择】向导页

❼ 在【许可协议】向导页中，仔细阅读许可协议条款，选中【我接受许可协议条款】单选按钮，单击【下一步】按钮继续，如图 7-32 所示。



图 7-32　【许可协议】向导页

❽ 在【选择更新源】向导页中，根据需要选择是否本地存储更新。如果选中【本地存储更新】复选框，则会将更新存储在 WSUS 3.0 服务器上，同时需要在文件系统中选择一个用于存储更新的位置。如果不在本地存储更新，客户端计算机将连接到 Microsoft Update 以获取已审批的更新。这里将存储更新位置设置为“D:\WSUS”，单击【下一步】按钮继续，如图 7-33 所示。

❾ 在【数据库选项】向导页中，选择用于管理 WSUS 3.0 数据库的软件。默认情况下，WSUS 安装程序将会安装 Windows Internal Database。如果不希望使用 Windows Internal Database，则必须为 WSUS 提供要使用的 SQL Server 实例，具体操作方法是：选中【使用此计算机上现有的数据库服务器】单选按钮，然后在框中输入实例名。此处设置实例名为 “<serverName>\ <instanceName>”，其中 serverName 是服务器的名称，instanceName 是 SQL 实例的名称。这里选中默认的【在此计算机上安装 Windows

Internal Database)】单选按钮，并将数据库文件存储在“D:\WSUS”文件夹中。选择好后单击【下一步】按钮继续，如图 7-34 所示。

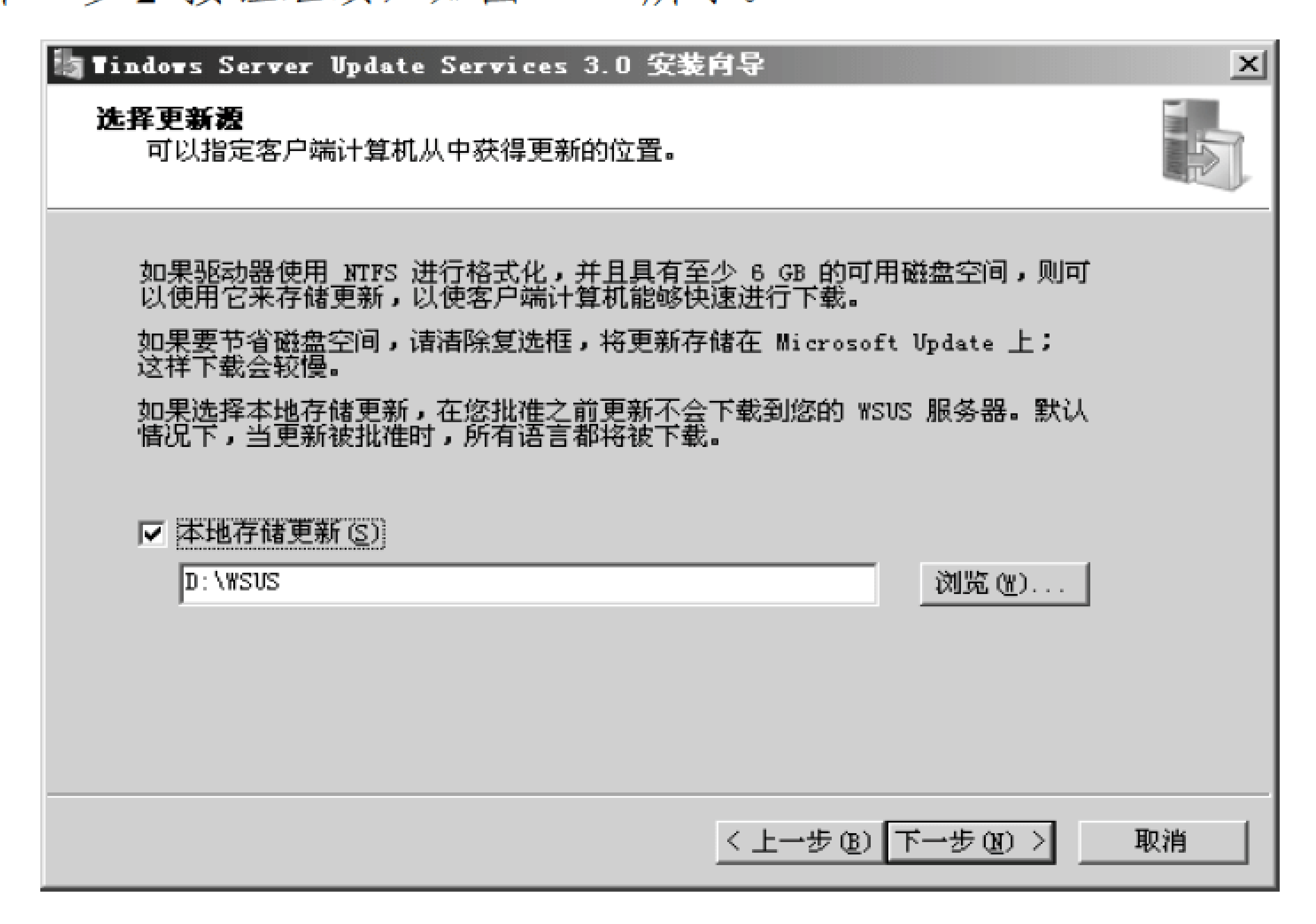


图 7-33　【选择更新源】向导页

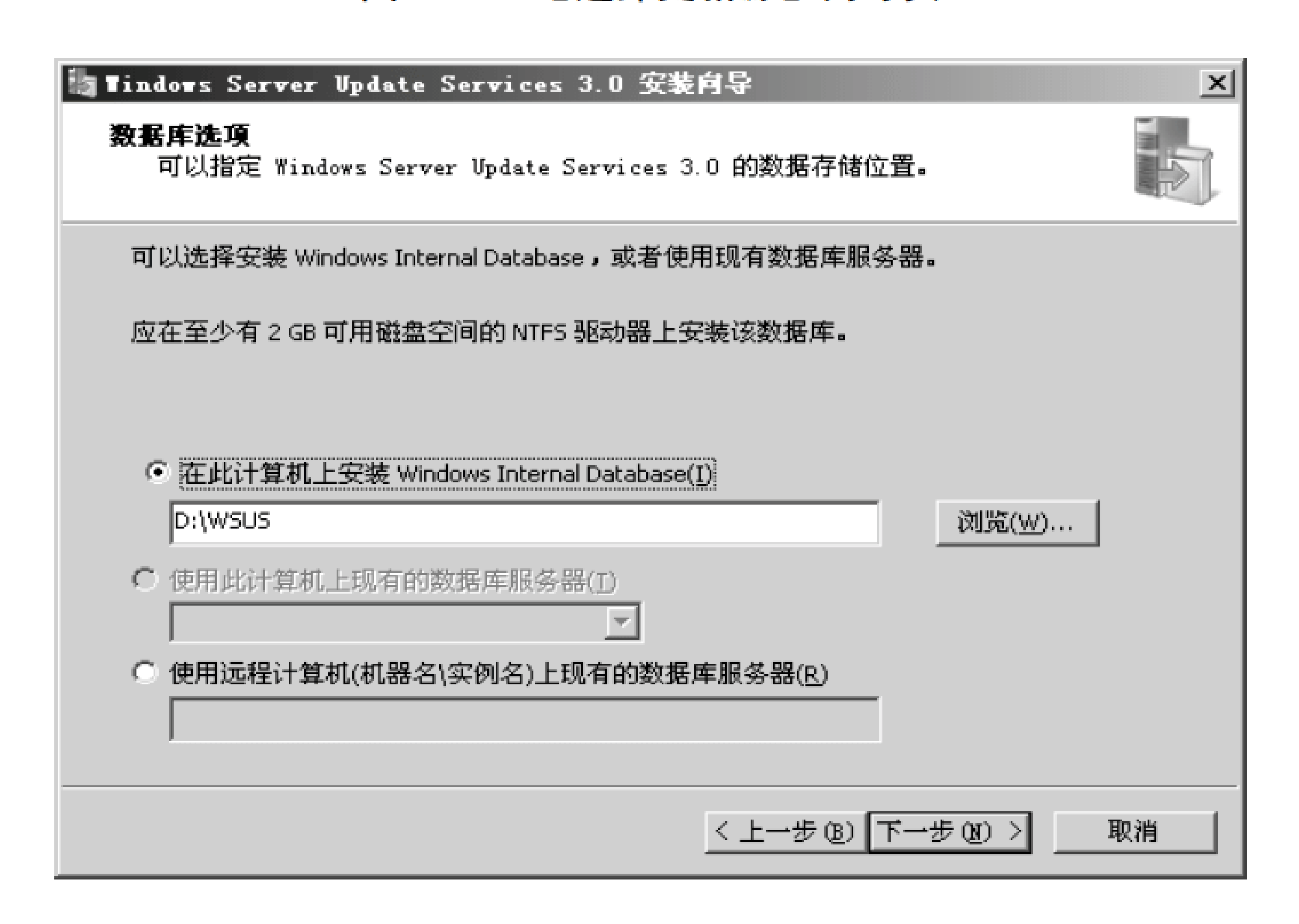


图 7-34　【数据库选项】向导页

⑩ 在【网站选择】向导页中，指定 WSUS 3.0 将使用的网站。如果要在端口 80 上使用默认 IIS 网站，请选中【使用现有 IIS 默认网站】单选按钮。如果端口 80 上已有一个网站，可通过选中【创举 Windows Server Update Service 3.0 网站】单选按钮，在端口 8530 上创建备用站点。这里使用默认设置，单击【下一步】按钮继续，如图 7-35 所示。

⑪ 在【准备安装 Windows Server Update Services 3.0】向导页中，显示前面配置的摘要，单击【下一步】按钮继续，如图 7-36 所示。

⑫ 此时，WSUS 开始进行安装，如图 7-37 所示。



图 7-35　【网站选择】向导页



图 7-36　【准备安装 Microsoft Windows Server Update Service】向导页



图 7-37　开始安装 WSUS

⓭ 安装向导的最后一页将说明 WSUS 3.0 安装是否成功完成。若安装成功，单击【完成】按钮后，将启动配置向导，如图 7-38 所示。至此，WSUS 服务器的安装就完成了。



图 7-38 WSUS 服务安装完成

7.2.3 配置 WSUS 服务器

安装 WSUS 3.0 服务器后，配置向导会自动启动；也可以稍后通过 WSUS 3.0 控制台窗口的【选项】界面来启动配置向导。通过配置向导配置 WSUS 服务器的过程如下。

❶ 配置向导启动后，在【在您开始之前】向导页中，提示管理员必须知道的几个问题的答案。默认情况下，将 WSUS 配置为使用 Microsoft Update 作为更新的获取位置。如果网络中具有代理服务器，则可以将 WSUS 配置为使用该代理服务器。如果 WSUS 和 Internet 之间设有企业防火墙，则可能需要配置防火墙以确保 WSUS 能够获取更新。单击【下一步】按钮继续，如图 7-39 所示。



图 7-39 【在您开始之前】向导页

❷ 在【加入 Microsoft Update 改善计划】向导页中，询问是否加入 Microsoft Update 改善

计划。这里不选中复选框表示不加入该计划，单击【下一步】按钮继续，如图 7-40 所示。

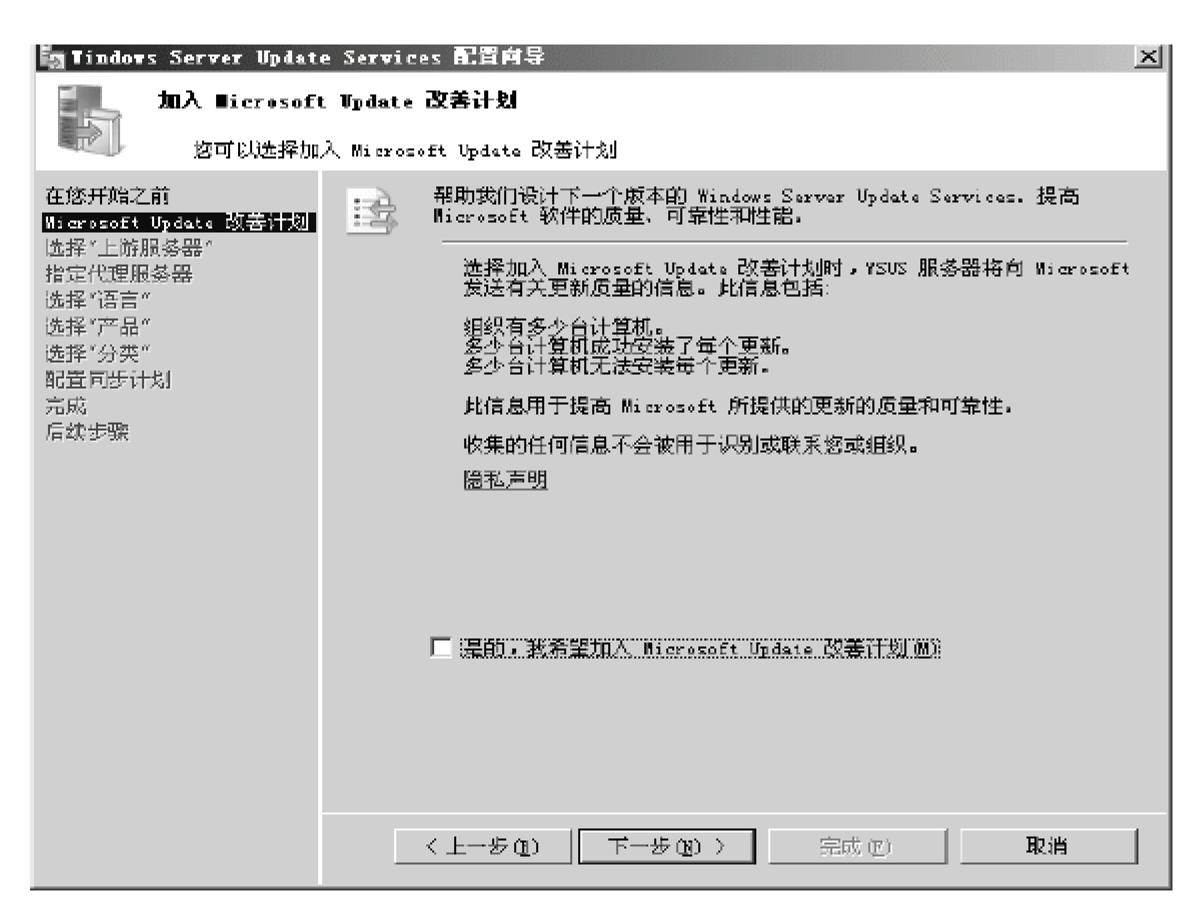


图 7-40　【加入 Microsoft Update 改善计划】向导页

❸ 在【选择“上游服务器”】向导页中，指定此服务器获取更新的方法，如图 7-41 所示。

✧ 如果选择从 Microsoft Update 进行同步，直接单击【下一步】按钮；
✧ 如果选择从另一台 WSUS 服务器进行同步，指定该服务器的名称及其与上游服务器进行通信所使用的端口；
✧ 如果要使用 SSL，则选中【在同步更新信息时使用 SSL】复选框。在这种情况下，服务器将使用端口 443 进行同步。此时要确保该服务器及上游服务器都支持 SSL；
✧ 如果这是副本服务器，则选中【这是上游服务器的副本】复选框。

这里选中【从 Microsoft Update 进行同步】单选按钮，单击【下一步】按钮继续。

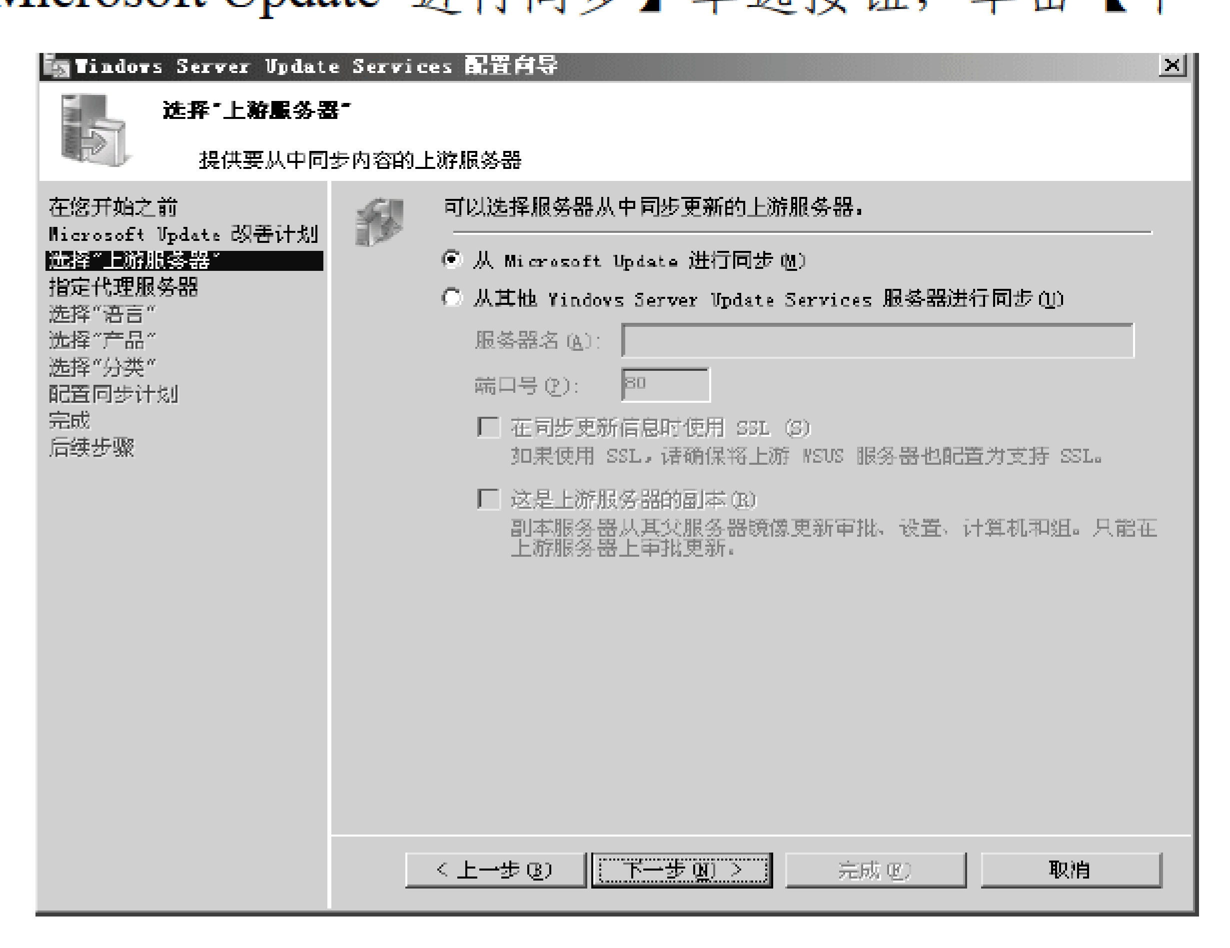


图 7-41　【选择“上游服务器”】向导页

❹ 在【指定代理服务器】向导页中，进行代理服务器设置，如图 7-42 所示。

✧ 如果此服务器能直接访问上游服务器，直接单击【下一步】按钮；

- ✧ 如果此服务器需要代理服务器才能访问上游服务器，则选中【在同步时使用代理服务器】复选框，然后在相应的框中输入代理服务器名和端口号(默认端口是 80);
- ✧ 如果要使用特定用户凭据连接到代理服务器，则选中【使用用户凭据连接到代理服务器】复选框，然后在相应的框中输入用户名、域和密码;
- ✧ 如果要为连接到代理服务器的用户启用基本身份验证，则选中【允许基本身份验证(以明文形式发送密码)】复选框。

在本例中，此服务器能直接访问上游服务器，单击【下一步】按钮继续。

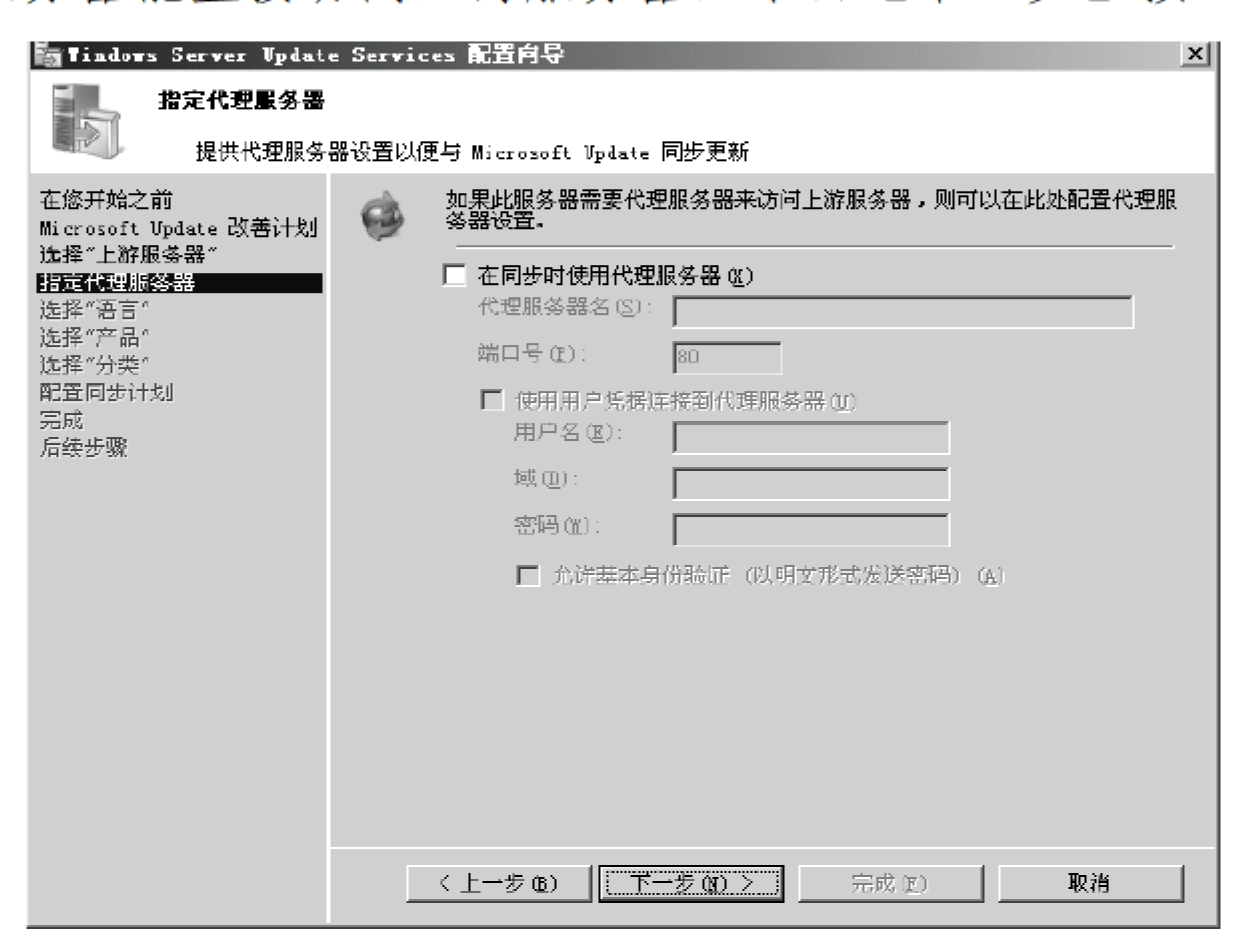


图 7-42 【指定代理服务器】向导页

5 在【连接到上游服务器】向导页中，保存和下载上游服务器和代理服务器信息，如图 7-43 所示。单击【开始连接】按钮，将会保存并下载设置以及获取有关可用更新的信息。当建立连接时，【停止连接】按钮将变为可用。如果连接出现问题，则单击【停止连接】按钮，解决该问题，然后重新启动该连接。在下载成功完成后，单击【下一步】按钮继续。



图 7-43 【连接到上游服务器】向导页

❻ 在【选择“语言”】向导页中，指定获取所有语言的更新或它的一个子集，如图 7-44 所示。选择一个语言子集会节省磁盘空间，但一定要选择此 WSUS 服务器的所有客户端将需要的所有语言。如果选择仅获取几种语言的更新，则选中【仅下载这些语言的更新】单选按钮，然后选择所需的更新语言复选框。这里仅选中【中文(简体)】复选框。单击【下一步】按钮继续。

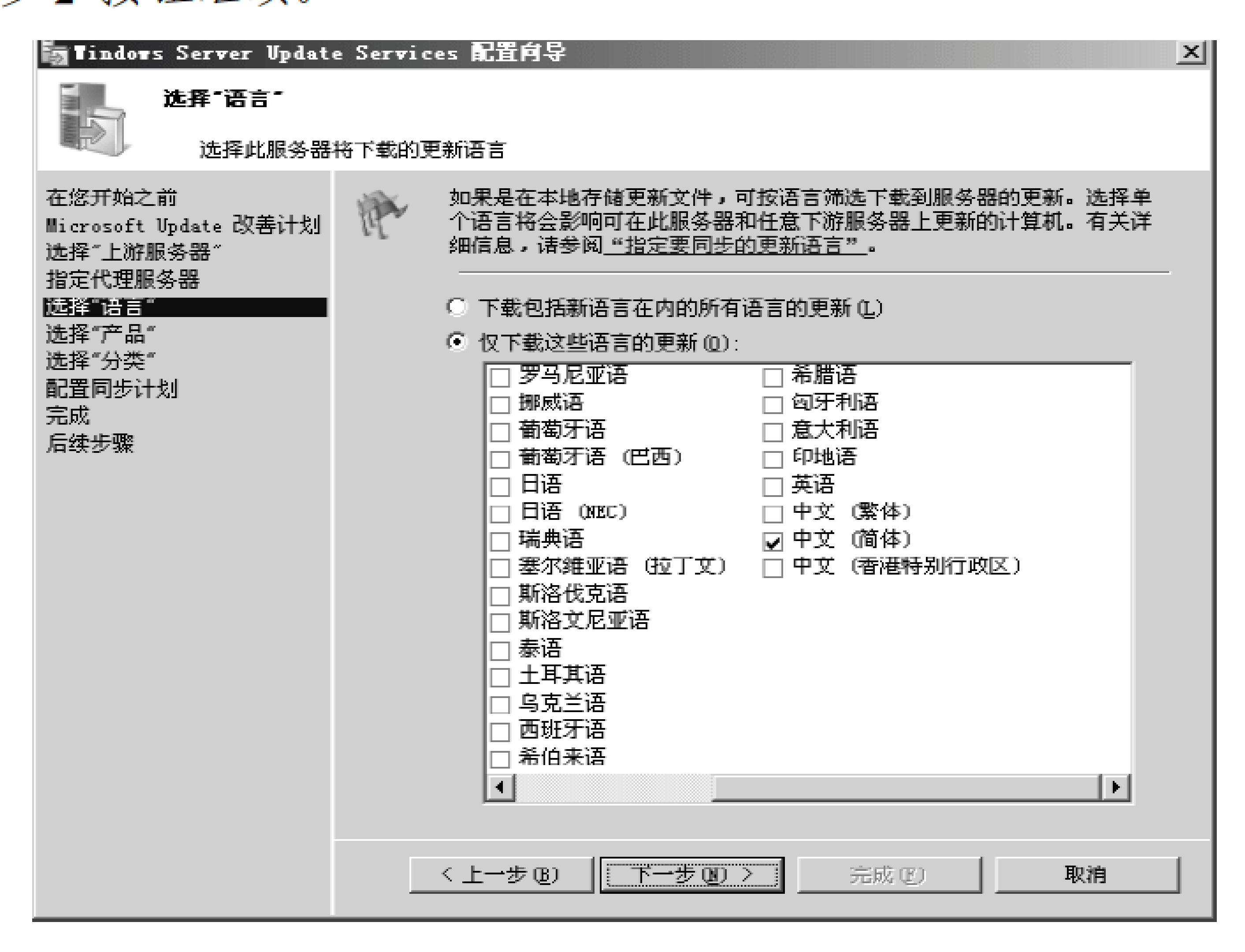


图 7-44　【选择“语言”】向导页

❼ 在【选择“产品”】向导页中，指定所需更新的产品，如图 7-45 所示。可以选中产品类别(如 Windows)或特定产品(如 Windows Server 2003)。选择产品类别后，单击【下一步】按钮继续。



图 7-45　【选择“产品”】向导页

❽ 在【选择“分类”】页中，选择要获取的更新分类。用户可以选择所有分类或它的一个子

集，这里仅选择 Service Pack、【安全更新程序】、【定义更新】和【更新程序】4 项。单击【下一步】按钮继续，如图 7-46 所示。



图 7-46 【选择"分类"】向导页

❾ 在【设置同步计划】向导页中，可以在其中选择手动执行同步，还是自动执行同步，如图 7-47 所示。如果选择在此服务器上手动执行同步，则必须从 WSUS 管理控制台中启动同步过程。如果选择自动执行同步，WSUS 服务器将按指定的时间间隔进行同步。这时需要设置首次进行同步的时间，并指定希望此服务器每天执行的同步次数。例如，如果指定每天同步 4 次并且从早晨 3:00 开始，则会在早晨 3:00、上午 9:00、下午 3:00 以及晚上 9:00 进行同步。配置完毕后，单击【下一步】按钮继续。

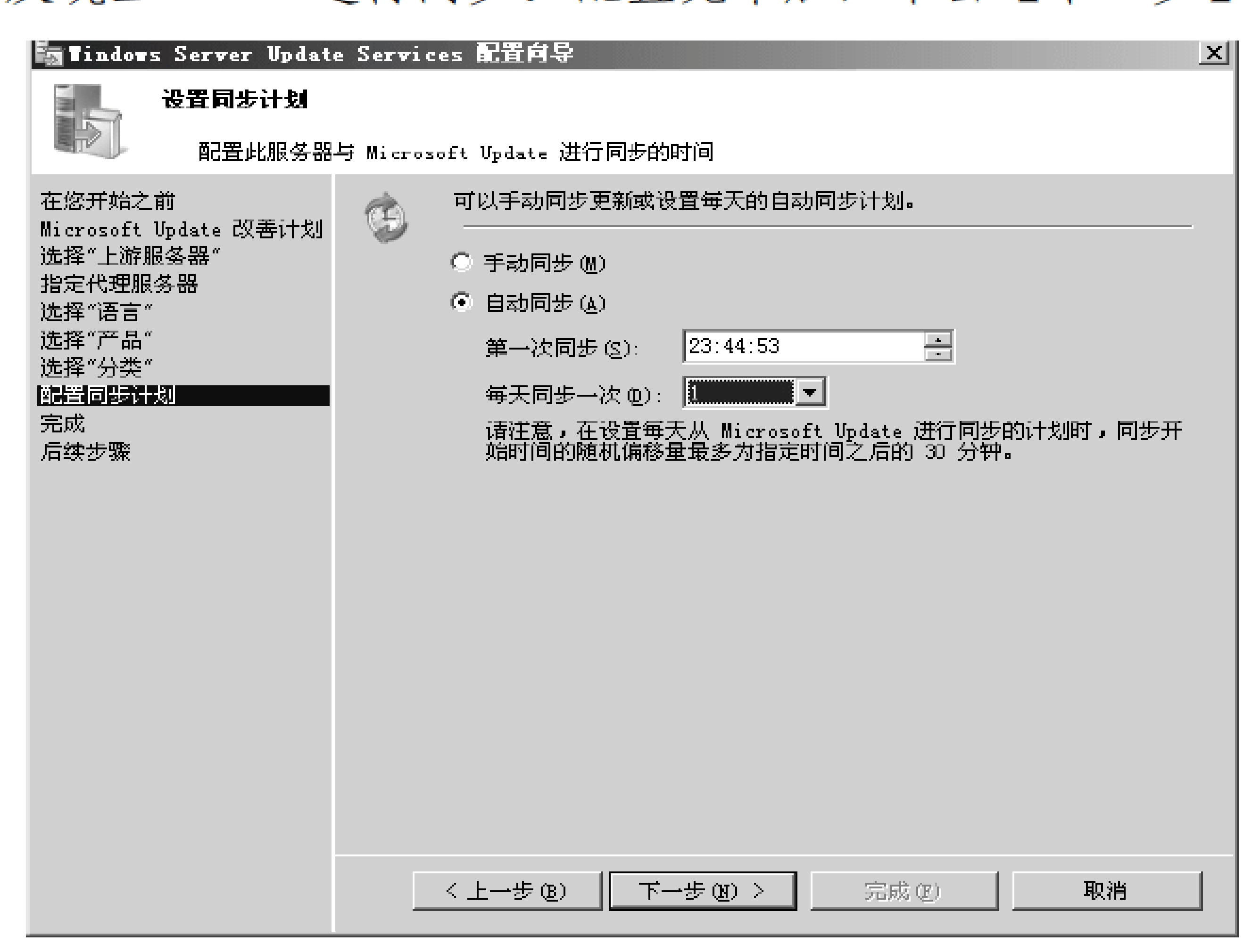


图 7-47 【设置同步计划】向导页

❿ 在完成所有以上配置后，进入【完成】向导页，如图 7-48 所示。可以选中【启动 Windows

Server Update Services 管理控制台】复选框来启动 WSUS 管理控制台，以及选中【开始初始同步】复选框来启动首次同步。配置完毕后，单击【完成】按钮关闭配置向导。

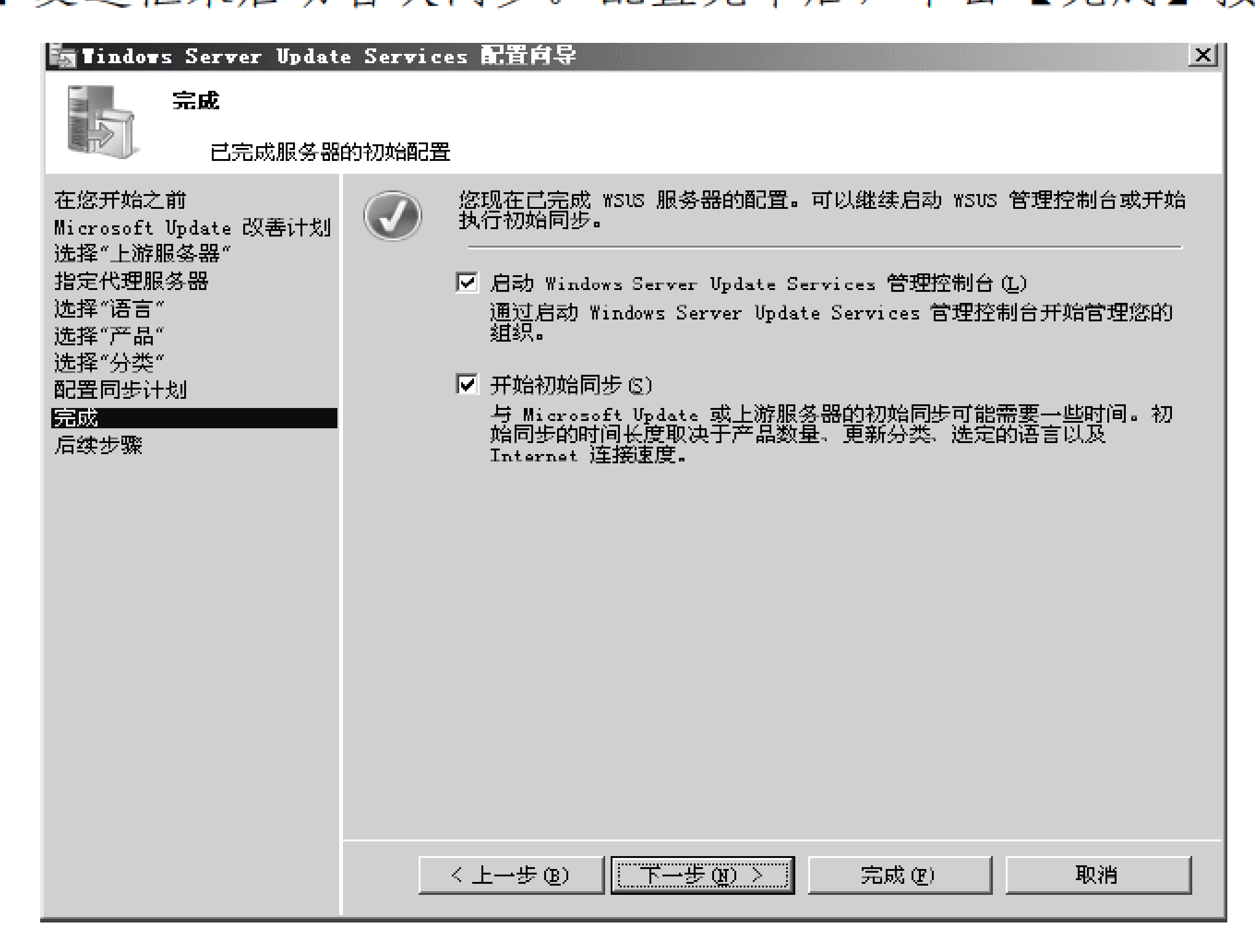


图 7-48　【完成配置】向导

7.2.4　配置 WSUS 客户端自动更新

自动更新是 WSUS 客户端软件。除网络连接外，自动更新无须任何特殊的硬件配置。在默认的情况下，WSUS 客户端是从 Windows Update 站点自动更新，如果要让客户端从上一节配置的 WSUS 服务器中自动更新，需要做一些配置。

配置 WSUS 客户端自动更新的操作方法取决于网络环境，在具有 Active Directory 的环境中，可以使用基于域的组策略对象(GPO)。在没有 Active Directory 的环境中，可以使用本地的 GPO。无论是使用本地的 GPO 还是使用基于域的 GPO，都必须先将客户端计算机指向 WSUS 服务器，然后才能配置自动更新。下面以在没有 Active Directory 的环境中为例，介绍 Windows XP Professional 自动更新的配置步骤。

❶ 在客户端计算机上，单击【开始】→【运行】命令，在【打开】下拉列表框中输入 gpedit.msc 命令，然后单击【确定】按钮，如图 7-49 所示。



图 7-49　打开本地组策略

❷ 在组策略对象编辑器中，依次选择【计算机配置】→【管理模板】→【Windows 组件】→Windows Update，如图 7-50 所示。



图 7-50 设置组策略

❸ 在右侧窗格中，双击【配置自动更新】。在弹出的对话框中选中【已启用】单选按钮，然后在【配置自动更新】下拉列表框中选择以下选项之一。

- ✧ 通知下载并通知安装：该选项在下载之前以及安装更新之前通知已登录的管理用户；
- ✧ 自动下载并通知安装：该选项自动开始下载更新，然后在安装更新之前通知已登录的管理用户；
- ✧ 自动下载并计划安装：如果将自动更新配置为执行计划安装，用户还必须设置执行定期计划安装的日期和时间；
- ✧ 允许本地管理员选择设置：如果选择该选项，则允许本地管理员使用【控制面板】中的【自动更新】来自行选择配置选项，例如可以选择自己的计划安装时间。不允许本地管理员禁用自动更新。

设置完毕后，单击【确定】按钮，如图 7-51 所示。



图 7-51 【配置自动更新 属性】对话框

❹ 在右侧窗格中，双击【指定 Intranet Microsoft 更新服务位置】。在弹出的对话框中选中

【已启用】单选按钮，然后在【为检测更新设置 Intranet 更新服务】文本框和【设置 Intranet 统计服务器】文本框中输入同一个 WSUS 服务器的 URL。例如，在两个文本框中输入“http://wsus.abc.edu.cn”。配置完毕后，单击【确定】按钮，如图 7-52 所示。



图 7-52　指定 Intranet Microsoft 更新服务位置

5 对于使用本地 GPO 配置的客户端计算机，将立即应用组策略，而刷新将需要大约 20 分钟的时间。在应用了组策略后，便可手动启动检测。如果手动启动检测，客户端计算机不必等待 20 分钟便可联系 WSUS。手动启动 WSUS 服务器检测方法是：在客户端计算机上，单击【开始】按钮，然后单击【运行】命令。在【打开】下拉列表框中输入 cmd，然后单击【确定】按钮。在命令提示符下，输入“wuauclt.exe /detectnow”。此命令行选项将指示自动更新立即联系 WSUS 服务器。

7.3　NAC 网络接入控制

7.3.1　终端安全接入概述

根据公安部最近公布的调查数据显示，内部网络的安全、计算机本身的安全仍是企业安全的关键。目前出现了几种安全接入技术，这些技术的主要思路是从终端着手，通过管理员来指定的安全策略对接入私有网络的主机进行安全性检测，自动拒绝不安全的主机接入来保护网络直到这些主机符合网络内的安全策略为止。目前具有代表性的技术主要有：思科的网络接入控制 NAC 技术、微软的网络接入保护 NAP 技术以及 TCG 组织的可信网络连接 TNC 技术等。

1. NAC 技术

网络接入控制(Network Access Control，NAC)技术是由 Cisco 公司主导的产业链协同研

究成果。NAC 可以协助保证每一个终端在进入网络前均符合网络安全策略。

在网络中部署 Cisco NAC 后，可完全依据组织内部已出台的安全策略来控制 PC、PDA 及服务器等端点设备对网络的访问。 Cisco NAC 拒绝不符合要求的设备访问网络，将其放置在隔离区或限制其对计算资源的访问。

2. NAP 技术

网络接入保护 (Network Access Protection，NAP) 技术是微软公司为其下一代操作系统 Windows Vista 和 Windows Server Longhorn 设计的新一套操作系统组件，它可以在访问私有网络时提供系统平台健康校验。NAP 平台提供了一套完整性校验的方法来判断接入网络的客户端的健康状态，对不符合健康策略需求的客户端限制其网络访问权限。

为了校验接入网络的主机的健康状态，网络架构需要提供以下功能性领域。

- ✧ 健康策略验证：判断计算机是否适应健康策略需求。
- ✧ 网络访问限制：限制不适应策略的计算机访问。
- ✧ 自动补救：为不适应策略的计算机提供必要的升级，使其适应健康策略。
- ✧ 动态适应：自动升级适应策略的计算机以使其可以跟上健康策略的更新。

3. TNC 技术

可信网络连接(Trusted NetworkConnection，TNC) 技术建立在基于主机的可信计算技术之上，其主要是通过使用可信主机提供的终端技术，实现网络访问控制的协同工作。由于完整性校验被终端作为安全状态的证明技术，所以用 TNC 的权限控制策略可以估算目标网络的终端适应度。TNC 网络架构会结合已存在的网络访问控制策略(例如 802.1x、IKE、RADIUS 协议)来实现访问控制功能。

TNC 架构主要是通过提供一个由多种协议规范组成的框架来实现一套多元的网络标准，它提供如下功能。

- ✧ 平台认证：用于验证网络访问请求者的身份以及平台的完整性状态。
- ✧ 终端策略授权：为终端的状态建立一个可信级别例如：确认应用程序的存在性、状态、升级情况，升级防病毒软件和 IDS 的规则库版本，终端操作系统和应用程序的补丁级别等，使终端被给予一个可以登录网络的权限策略从而获得在一定权限控制下的网络访问权。
- ✧ 访问策略：确认终端机器及其用户的权限，并在其连接网络以前建立可信级别，平衡已存在的标准、产品及技术。
- ✧ 评估、隔离及补救：确认不符合可信策略需求的终端机能被隔离在可信网络之外，如果可能执行适合的补救措施。

7.3.2 Cisco NAC 概述

NAC 是一项 Cisco 发起的、多家厂商参加的计划，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成的危害。Cisco NAC 解决方案包括 NAC Appliance 和 NAC Framework 两种模式。

1. NAC Appliance

NAC Appliance 由 Cisco Clean Access 系列产品构成(如图 7-53 所示)，它包括 CAM(Clean Access Manager)、CAS(Clean Access Server)和 CAA Agent(Clean Access Agent)3 个产品。

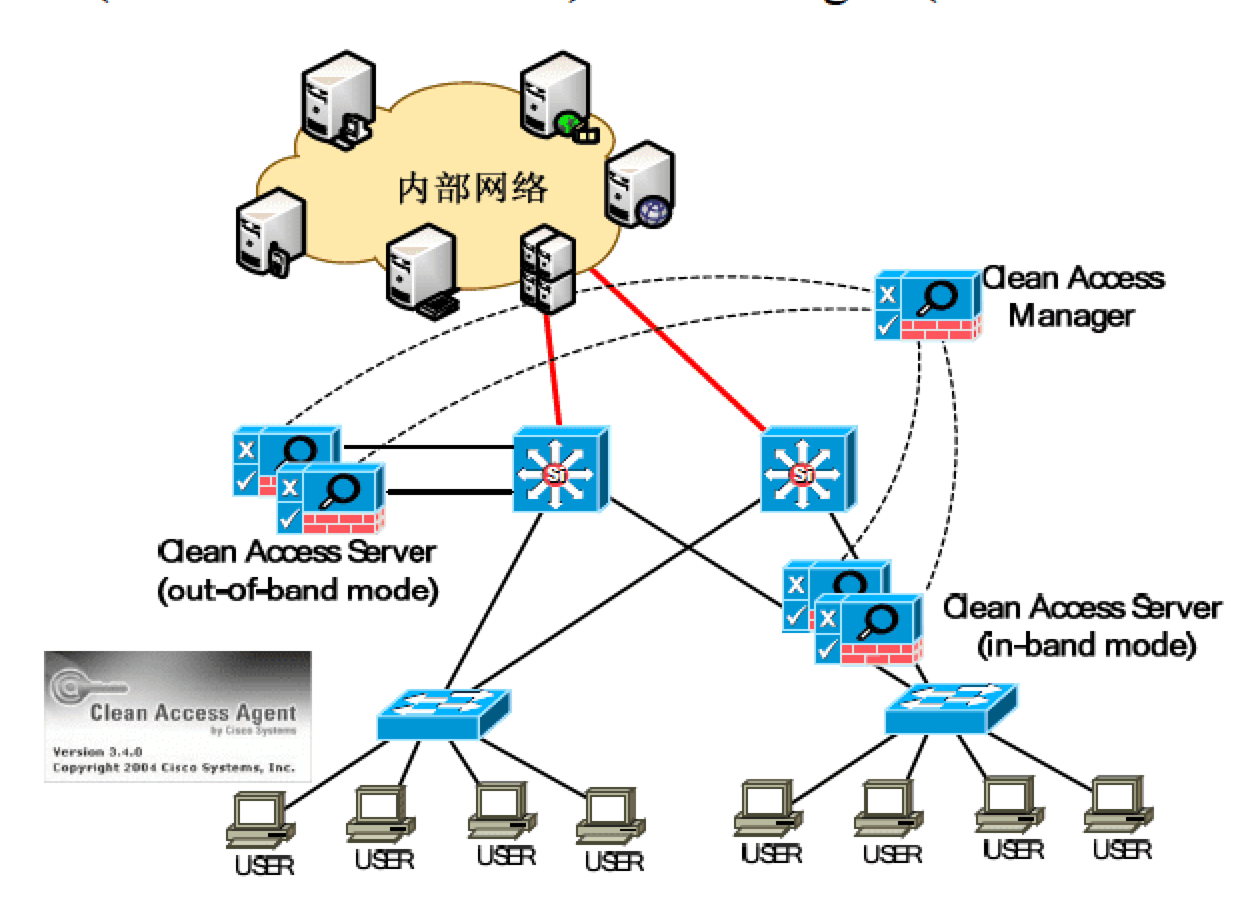


图 7-53　Cisco NAC Appliance

- ✧ CAM：CAS 部署策略，集中管理 CAS，接受来自 CAS 的用户检查报告并进行分析，告知 CAS 用户的健康状况。
- ✧ CAS：接受 CAM 的管理，拦截用户 HTTP 请求重新定向，进行 Network Scanning，收集 CAA Agent 信息等功能，并发送给 CAM 分析；根据 CAM 检查结果，对于接入用户分配 ACL 限制，或者利用 SNMP 方式通知交换机对用户进行相应的 VLAN 分配操作。
- ✧ CAA Agent：用于客户端的轻量级软件，用于收集客户机相关信息，如 Hotfix、AV、Anti-spware 等。

在图 7-53 中，NAC Application 支持 CAS 使用串接(in-band)或者旁挂(out-of-band)两种方式连接。通常，串接方式用于无线基站、VOIP 电话、媒体流共享等服务使用；而旁挂方式则用于快速的核心交换机和吞吐量较高的网络使用，并且仅支持 Cisco 的交换机平台。

Cisco Clean Access 使用两种机制对客户机状态进行检测。

- ✧ Network Scanning：通过集成第三方脆弱性扫描工具实现对于客户端的健康状态检查，基于检查结果对客户机采取相应的准入控制策略。此方法部署简单，无须客户端安装其他检测程序。
- ✧ 在客户端上安装 CAA Agent：由 CAA Agent 收集客户机相关信息(如 Hotfix、AV、Anti-spware 等)来确定主机的健康状态。基于检查结果对客户机采取相应的准入控制策略。此方式可以与 Network Scanning 集成使用，两者同时启用的情况下，认证为逻辑 AND 的关系，基于两者检查结果对客户机采取相应的准入控制策略。

2. NAC Framework

NAC Framework 是最初的安全解决方案，它由网络接入设备、Cisco 可信代理(Cisco

Trust Agent，CTA)、Cisco 策略/AAA 服务器(Cisco Secure ACS)、Cisco 安全代理(Cisco Security Agent，CSA)以及第三方的反病毒策略服务器构成。通常 NAC 有 3 种部署方式。

- ✧ L2-dot1x：用户需要首先进行 802.1x 认证，在认证过程中通过 EAP-FAST 进行状态确认，ACS 根据检查后的结果为用户分配不同的 VLAN，它通过 EAPo802.1x 控制，Cisco 2900 系列以上交换机都支持这种部署方式。
- ✧ L2-IP：用户不需要做接入认证，系统通过 PEAP 对终端进行状态确认，确认后将针对每个 IP 的 DACL 下载到交换机；它通过 EAPoUDP 控制，Cisco 3550 系列以上交换机支持这种部署方式。
- ✧ L3-IP：在三层设备(如 Router 或 VPN Gateway)上做状态检查和策略执行，它通过 EAPoUDP 控制，Cisco800 以上路由器及 VPN Concentrator 3000 支持这种部署方式。

一个常见的 NAC Framework 拓扑结构如图 7-54 所示。

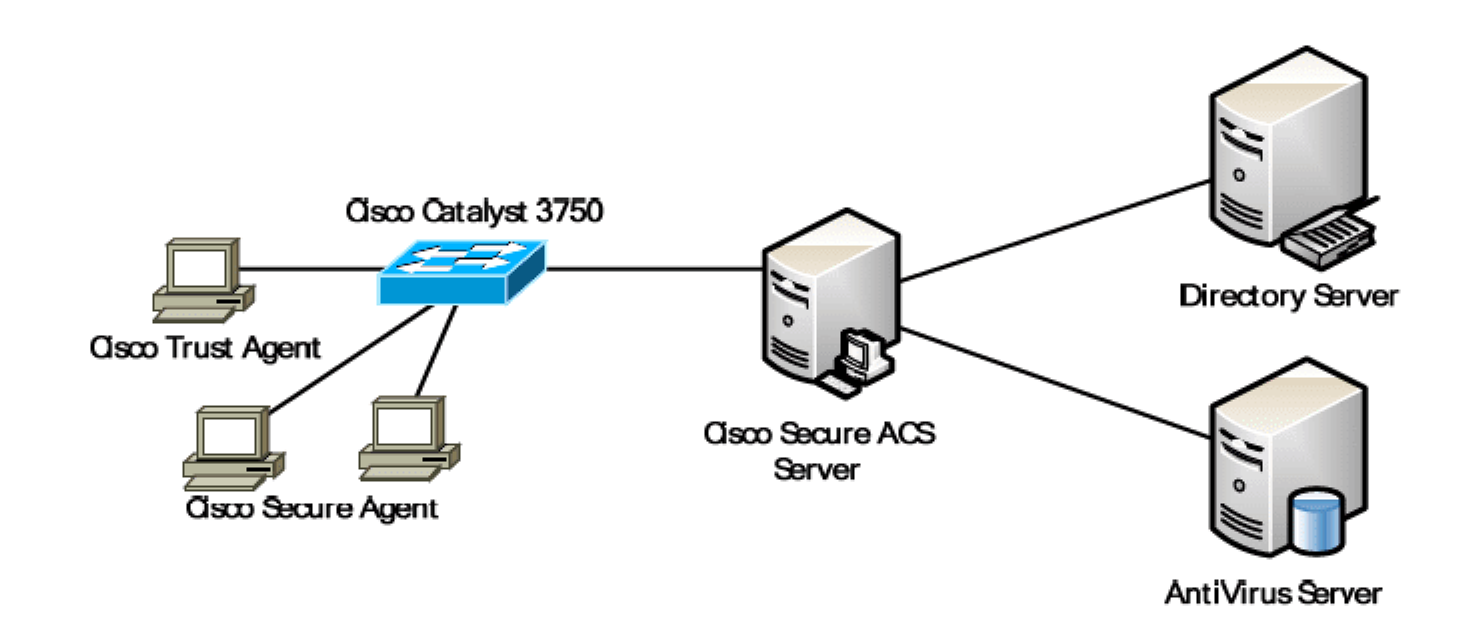


图 7-54　Cisco NAC Framework

首先 CTA 将身份认证信息和主机安全信息发送给交换机，然后交换机将认证信息转发给 ACS；ACS 收到信息开始处理并与目录服务器交互，确认用户权限；然后 ACS 检查入网计算机 Service Pack、Hotfix 以及 CSA 版本等信息，并与第三方反病毒策略服务器进行交互，确认用户的健康状况；此后根据反病毒策略服务器以及 AD 服务器的信息，判断是否通过认证，并根据验证信息向交换机发送相应的 VLAN 及 ACL 信息；最后将认证结果告知 CTA。

通常在全网都为 Cisco 设备的情况下，使用 NAC Framework 相对简单并且成本低廉；而如果网络中有很多的第三方设备，则需要使用 NAC Appliance 进行配置。

7.3.3　配置 Cisco NAC

在本章开始的时候已经介绍了基于 AD 和 Cisco Secure ACS 的统一身份认证来实现 802.1x 访问控制。因此我们将从这样的架构升级到 L2-dot1x NAC Framework。所需的配置组件如下。

- ✧ Cisco Secure ACS v4.0
- ✧ Microsoft CA and Active Directory　　//用于统一身份认证
- ✧ Trend Micro OfficeScan v7.0　　//第三方杀毒软件

下面简单地介绍升级 L2-dot1x NAC Framework 的配置过程，主要过程包括配置 Cisco Secure ACS、在接入交换机上配置 NAC L2-dot1x、安装并配置 Trend Micro OfficeScan 第三

方杀毒软，件以及在客户端上安装 Cisco Trust Agent。

1. 配置 ACS

将 802.1x 访问控制架构升级到 L2-dot1x NAC Framework 架构时，需要对 RADIUS 服务器 Cisco Secure ACS 进行进一步的配置，其操作步骤大致如下。

❶ 按照 7.1 节的方法配置基于 AD 的 802.1x 认证，然后将第三方软件供应商的 ADF 文件复制到 ACS 服务器上。以 Trend Micro 为例，其名称一般为 Trendavp.adf。首先在 ACS 服务器中进入 ACS 安装目录，假设 ACS 安装在系统 C 盘，则进入 C:\Program Files\CiscoSecure ACS v4.0\bin，运行如下命令。

```
C:\Program Files\CiscoSeure ACS v4.0\bin>CSUtil.exe -addAVP C:\Trendavp.adf
```

❷ 配置内部状态确认。依次单击 Posture Validation →Internal Posture Validation Setup 链接，再单击 Add Policy 按钮增加一个 Policy(策略)，输入名称和说明信息后，单击 Submit 按钮，如图 7-55 所示。

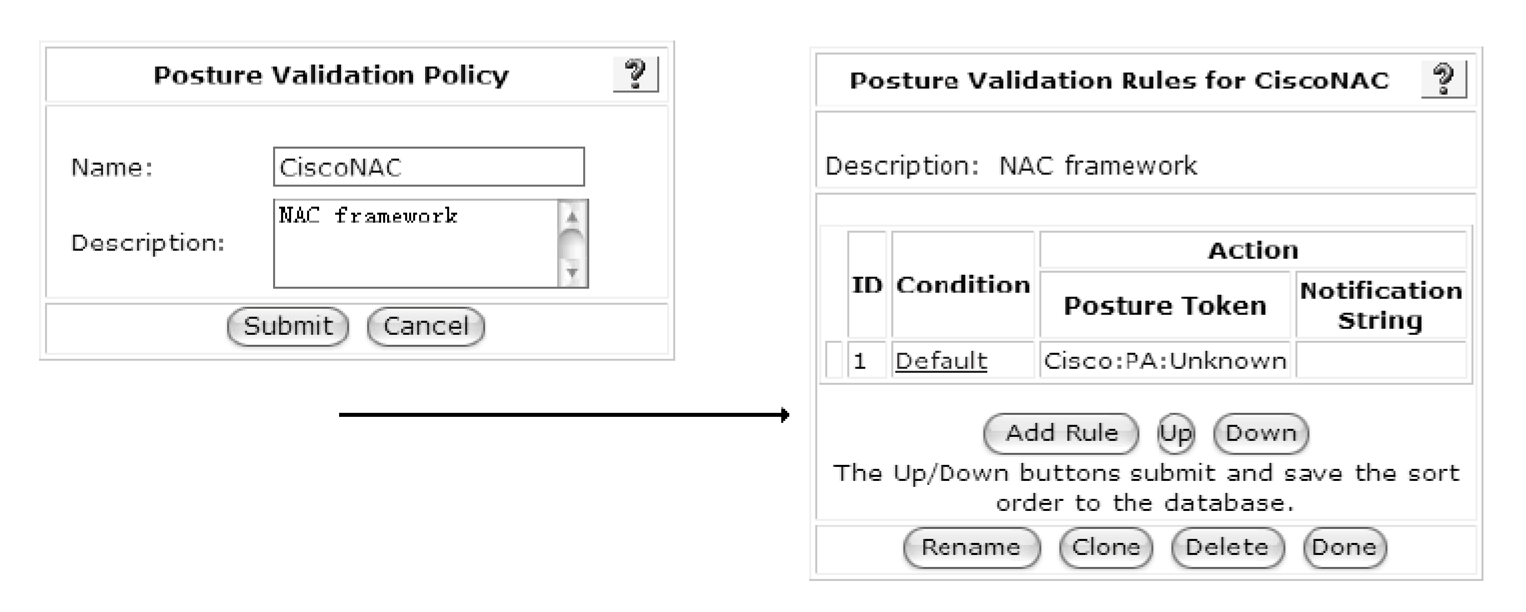


图 7-55　增加 Posture validation Policy

❸ 增加 Policy 后，还需要增加新 Rule(规则)。单击 Add Rule 按钮，在 Rule 配置中单击 Add Condition Set 按钮增加 Condition Set(条件集)，并在 Condition Set 配置中按照预定策略进行配置(可以配置多个 Condition)，最后在 Rule 配置中选择 Condition 内部和 Condition 之间的关系(即 OR 或 AND)，如图 7-56 所示。

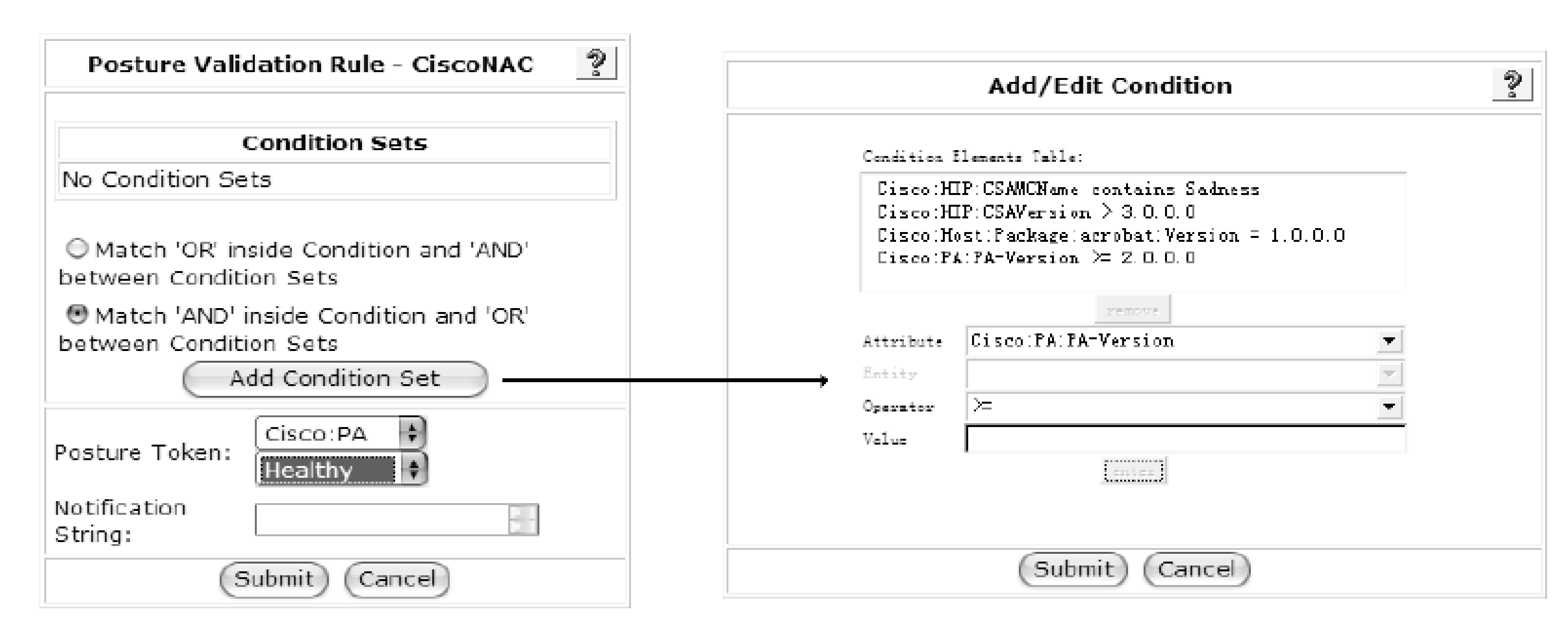


图 7-56　添加 Rule

❹ 依次选择 System Configuration →Global Authentication Configuration→EAP-FAST Configuration 命令，对 EAP-FAST 进行配置，如图 7-57 所示。

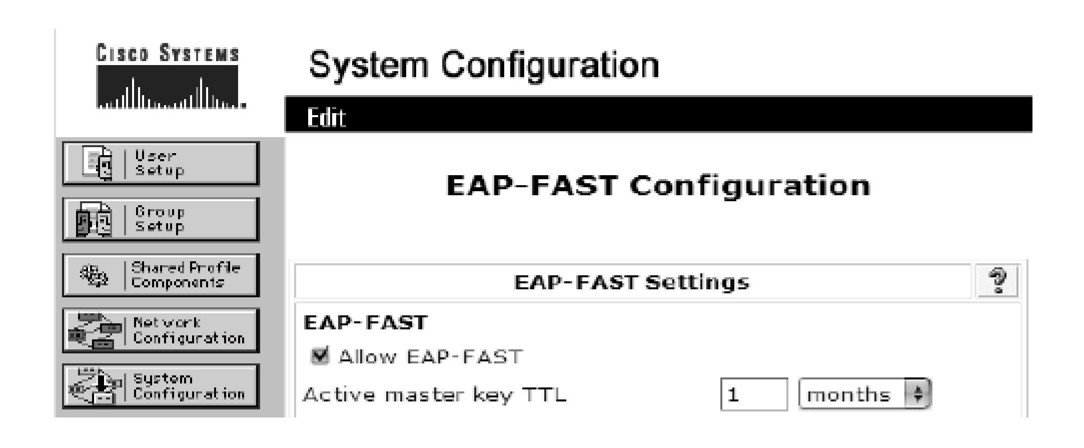


图 7-57　配置 EAP-FAST

❺ 添加新的 RAC。依次选择 Shared Profile Components →RADIUS Authorization Components 命令，单击 Add 按钮，如图 7-58 所示。在 L2-dot1x 配置中，至少需要两种 RAC，一种是健康的(系统默认命名为 Healthy)，一种是非健康的(系统默认名为 Quarantine)。在 RAC 内部加入相应的 Attributes。对于 L2-dot1x，需要配置的 Attributes 有：Cisco-av-pair、Tunnel-Private-Group-ID、Termination-Action、Session-Timeout、Tunnel-Type、Tunnel-Medium-Type (必须与 Switch 中 VLAN 名称的配置一样)。

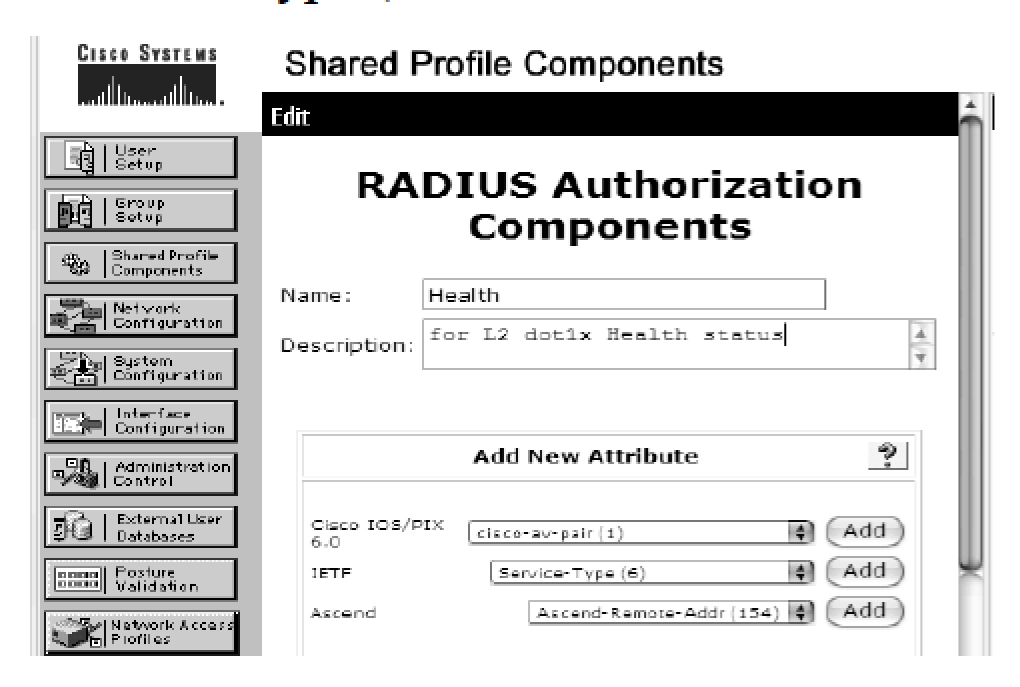


图 7-58　添加 RAC

❻ 配置访问控制列表(ACL)只允许访问 WSUS 和 Anti-virus 服务器，而拒绝其他连接。依次选择 Interface Configuration→Advanced Options 命令，选中 User-Level Downloadable ACLs 复选框，并单击 Submit 按钮。再依次选择 Shared Profile Components→Downloadable IP ACLs 命令，单击 Add 按钮；输入 ACL 的名称和说明后单击 Add 按钮，如图 7-59 所示。

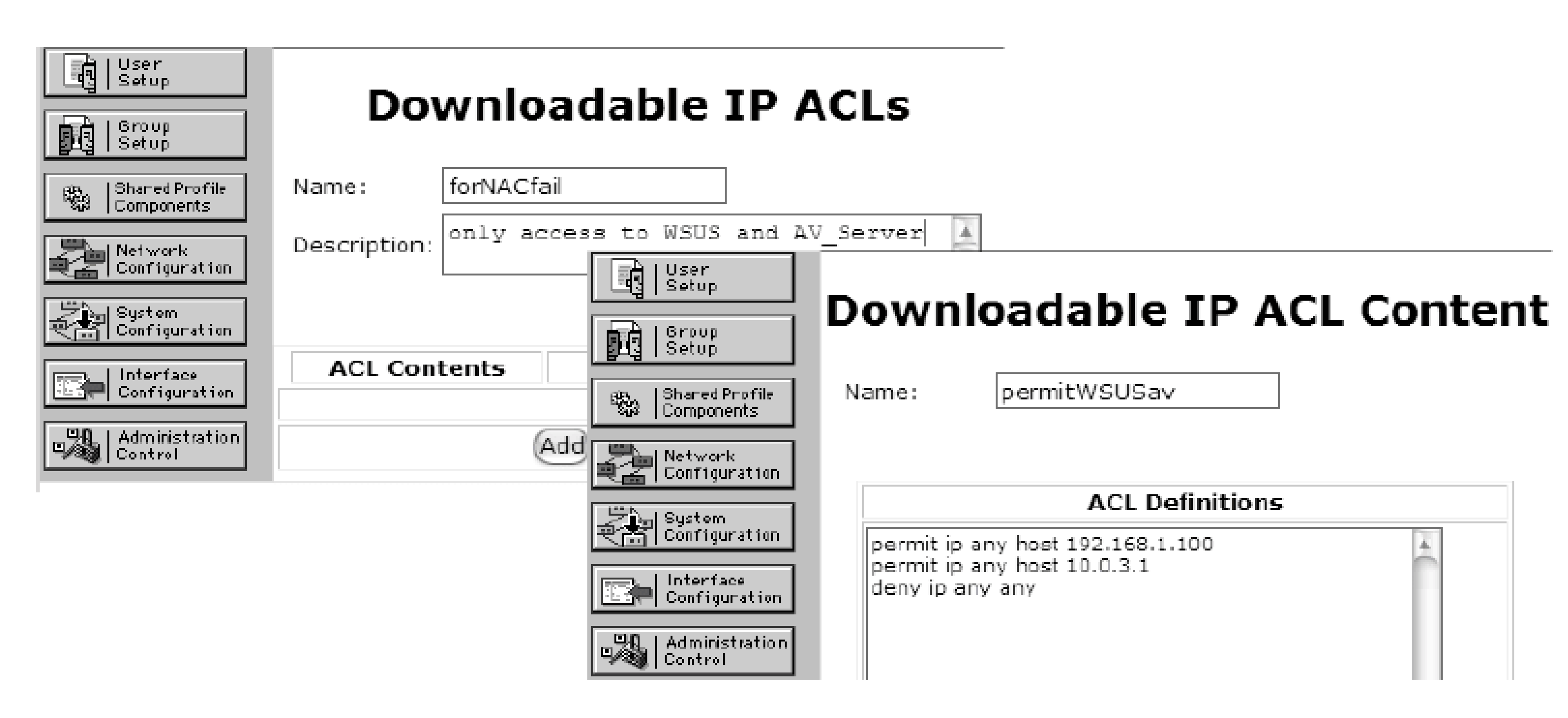


图 7-59　添加 Downloadabe ACL

❼ 添加网络接入策略(NAP)。单击 Network Access Profiles 按钮，选择 Add Profile 添加一个 NAP，并在 NAP Name 配置中关联相应的 NAF。完成配置后，将出现如图 7-60 所示的界面。



图 7-60　添加 NAP 后的界面

❽ 配置认证类型。单击 Authentication 按钮，选中 Allow EAP-FAST 复选框；对于网络打印机等设备，还需要同时选中 Allow MAC-Authentication By pass 复选框，并将不支持 802.1x 的可信任设备 MAC 地址加入其中，如图 7-61 所示。

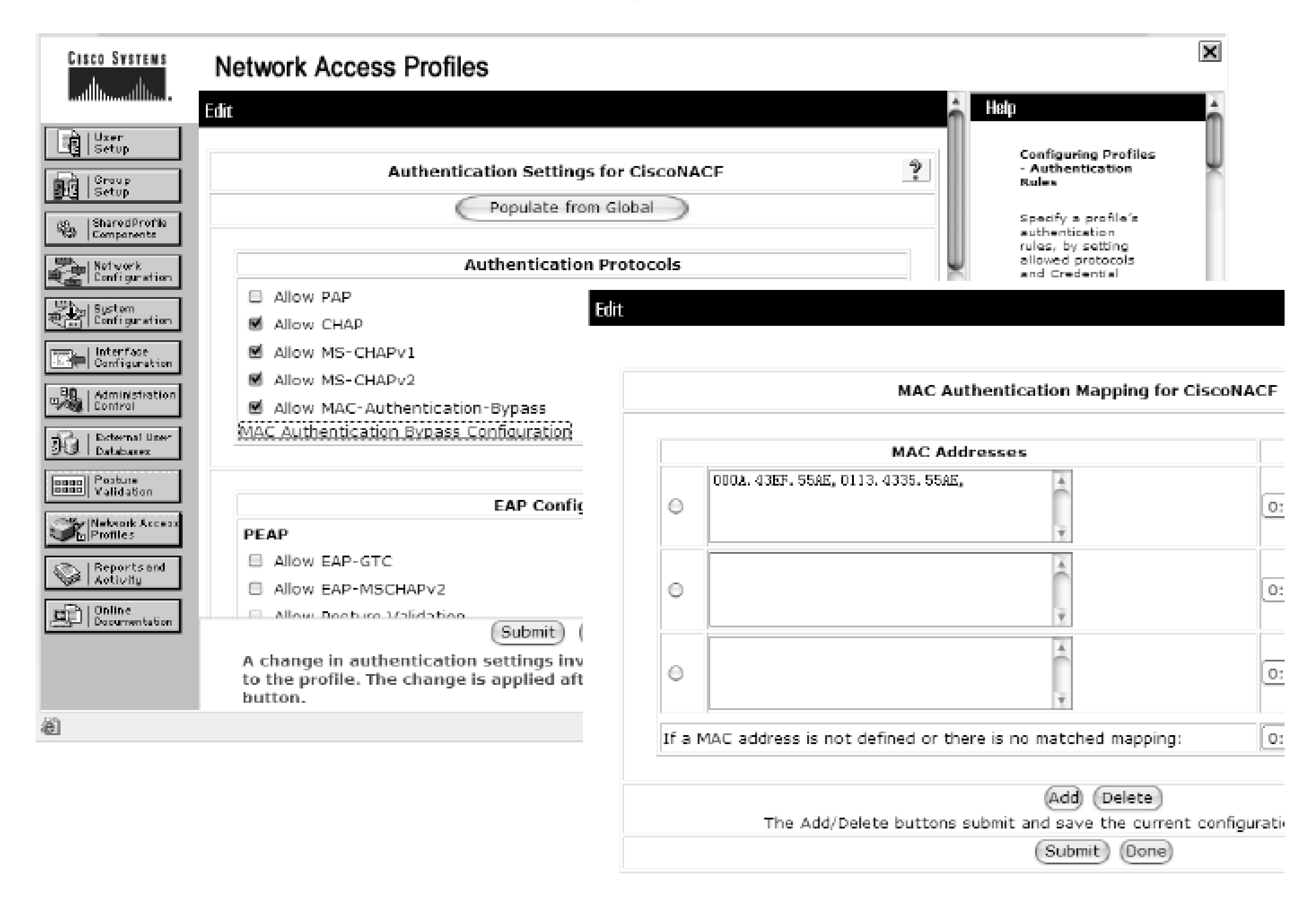


图 7-61　配置 MAC Authentication

❾ 添加新规则。单击 Posture Validation 按钮，单击 Add Rule 按钮添加一条 Rule(规则)。配置完 Rule 后，单击 Submit 按钮，如图 7-62 所示。

❿ 在 Condition 项中添加需要检查的 Credential Types，系统默认有 3 个：Cisco:Host、Cisco:HIP 和 Cisco:PA。当引入 ADF 后，会添加相应选项，例如 Symantec:AV、NAI:AV 和 Trend:AV 等。

✧ Action：选中在 Posture Validation 中预先定义好的 Validation Policies;

✧ Assessment Result Configuration：对不同的 Assessment Result 配置不同的 PA Message，并使用 URL 重定向功能用来提醒用户；

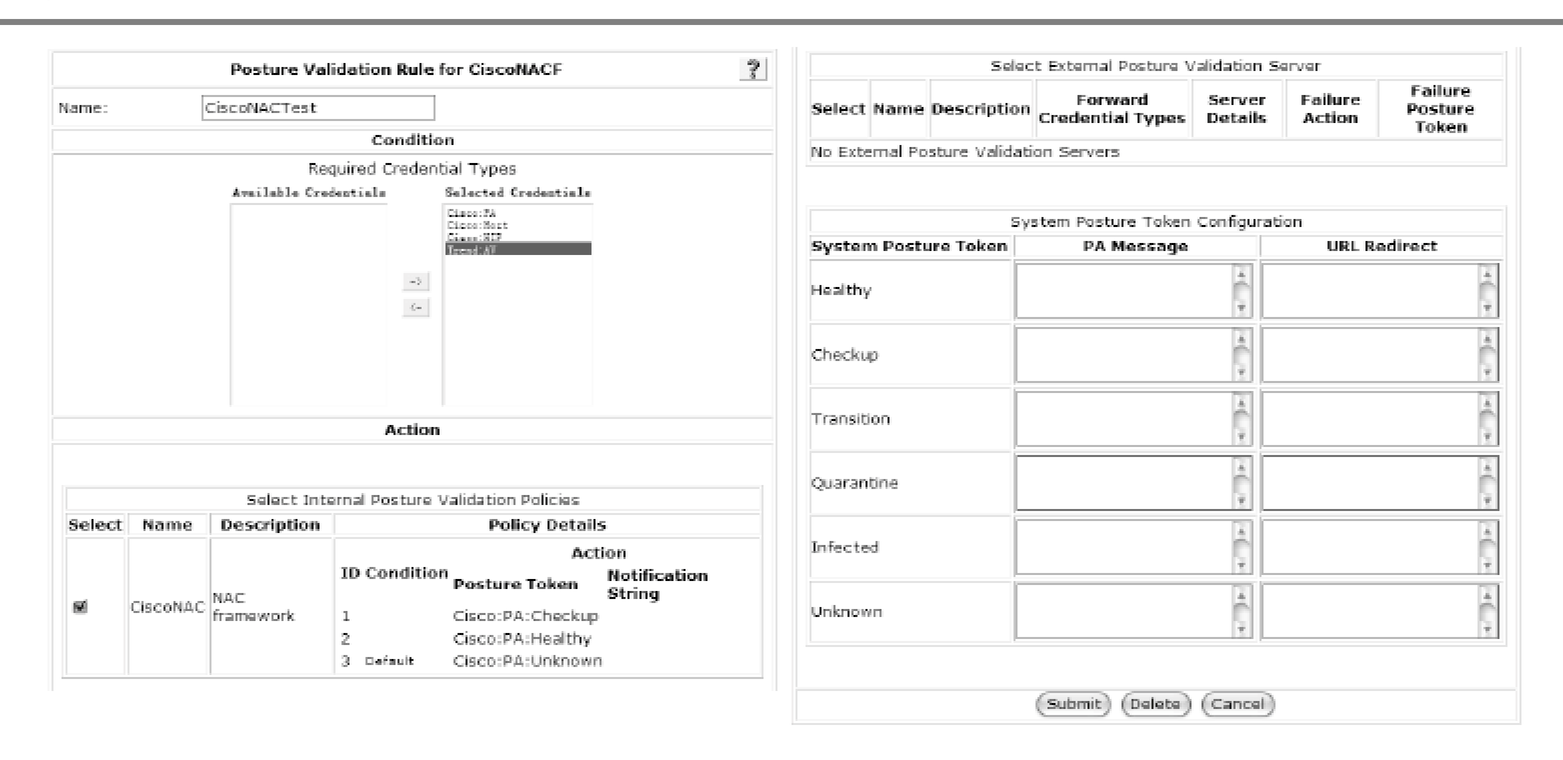


图 7-62　配置 NAP Posture Validation

✧ Authorization：在每一行配置中，选择认证用户组、评估结果，以及根据这个结果需要执行的 RAC，并配置相应的 Downloadable ACL，使得认证失败后的主机仅能访问 Windows 更新服务器以及 Anti-Virus Server 杀毒，如图 7-63 所示。

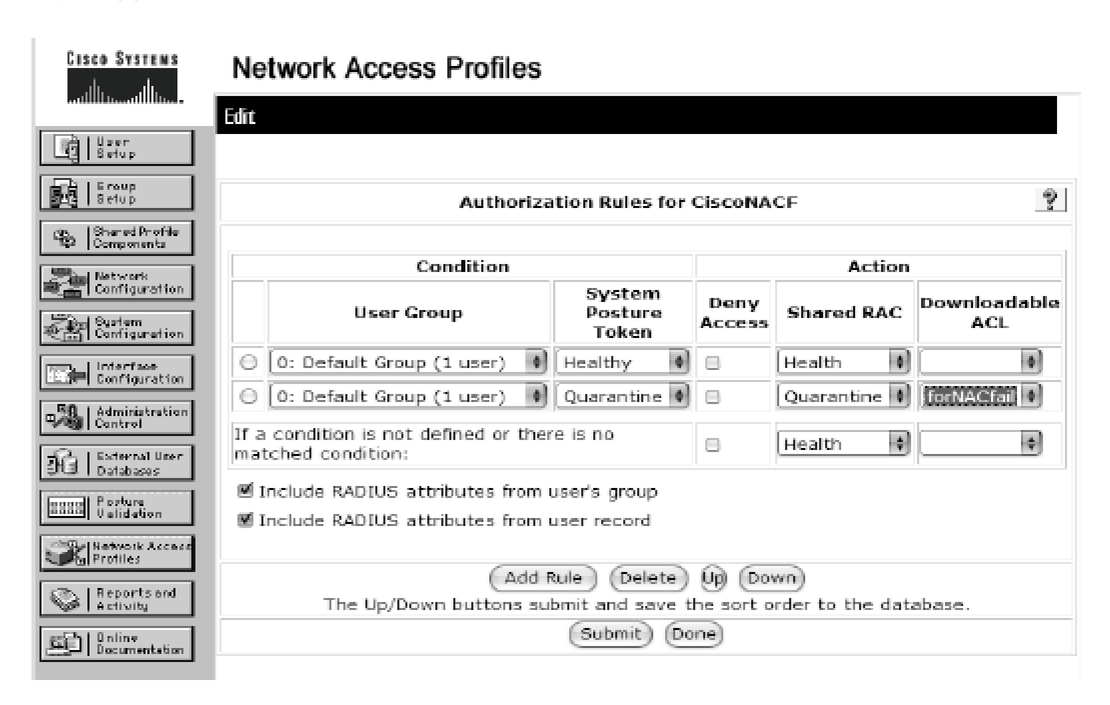


图 7-63　配置 Authorization Rules

⓫ 依次选择 System Configuration→Logging 命令，配置记录日志，如图 7-64 所示。

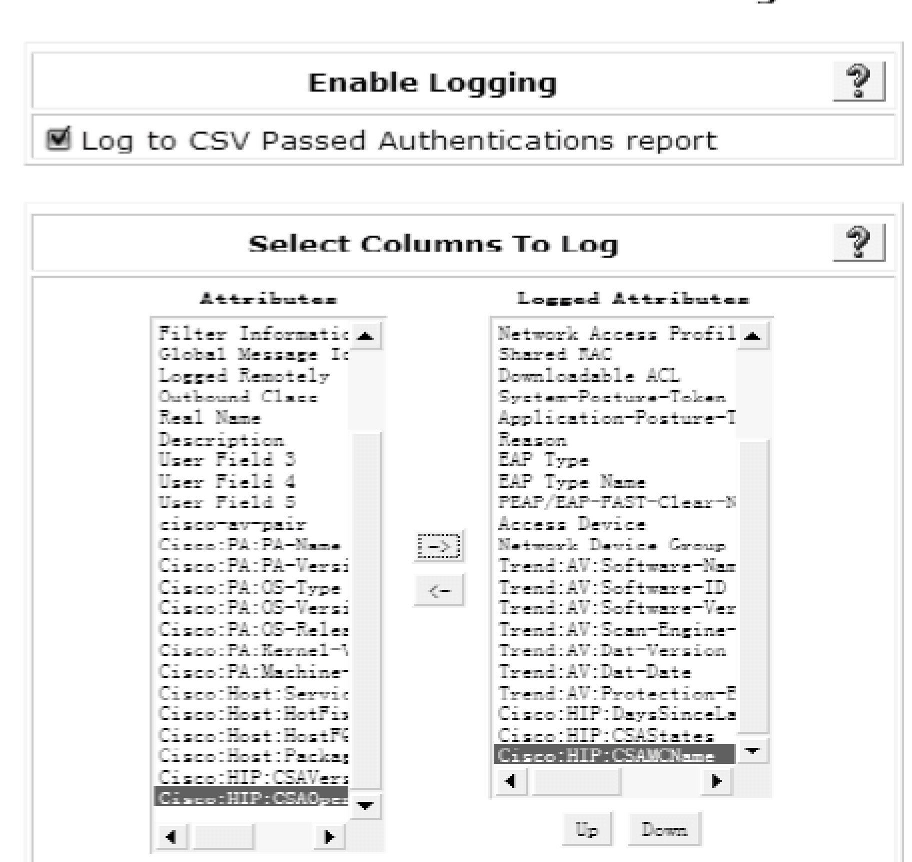


图 7-64　配置系统日志

⓬ 为 ACS 上配置外部策略服务器。方法是依次选择 Posture Validation→External Posture Validation Setup→Add Server 命令，如图 7-65 所示。

注意，TM Policy Server 访问 URL 按照如下格式填写。

```
https://192.168.1.101:4344/antibody/cgi-bin/PostureRequest.dll?PostureRe
quest
IP 地址：Trend Micro Policy服务器地址
端口号：Trend Micro Policy服务器访问端口， 默认4344
如果使用http直接连接，则URL为：
http://192.168.1.101:8081/antibody/cgi-bin/PostureRequest.dll?PostureReq
uest
默认端口8081
```

图 7-65　配置外部策略服务器

2. 配置 NAC L2-dot1x

Cisco Secure ACS 配置完成后，还需要在接入交换机上配置 NAC L2-dot1x，其方法如下。

❶ 在交换机中定义两个 VLAN，例如符合网络准入策略的用户进入用户 VLAN(VLAN100)，而不符合网络准入策略的用户进入 VLAN 200。注意，VLAN 名称需要和 ACS 中 RAC 一致。

```
Switch(config)#vlan 100
Switch(config-vlan)#name Health
Switch(config)#vlan 200
Switch(config-vlan)#name Qurantine
```

❷ 按照第 6 章介绍，配置 AAA 及 RADIUS 服务器。

```
Switch(config)#aaa newmodel
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network default group radius
Switch(config)#aaa authorization cache filterserver radius
Switch(config)#aaa accouting network default start-stop group radius
Switch(config)#radius-server host 192.168.1.101 key Cisco
Switch(config)#radius-server vsa send authentication
```

❸ 在全局配置模式下，全局启用 dot1x 认证。

```
Switch(config)#dot1x systemauthcontrol
```

❹ 在需要实施终端安全接入控制的端口中启用 dot1x 认证。

```
Switch(config)#Interface  fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#spanning-tree portfast
```

3. 安装并配置第三方杀毒软件

下面以 Trend Micro OfficeScan V7.0 为例，介绍在 L2-dot1x NAC Framework 架构中第三方杀毒软件的安装与配置方法。

❶ 在安装 Trend Micro OfficeScan V7.0 之前，需要确保已经安装 IIS 或 Apache 等 Web 服务器。

❷ 在 Trend Micro OfficeScan V7.0 安装过程中，需要选中 Install Policy Server for Cisco NAC 复选框 ，如图 7-66 所示。

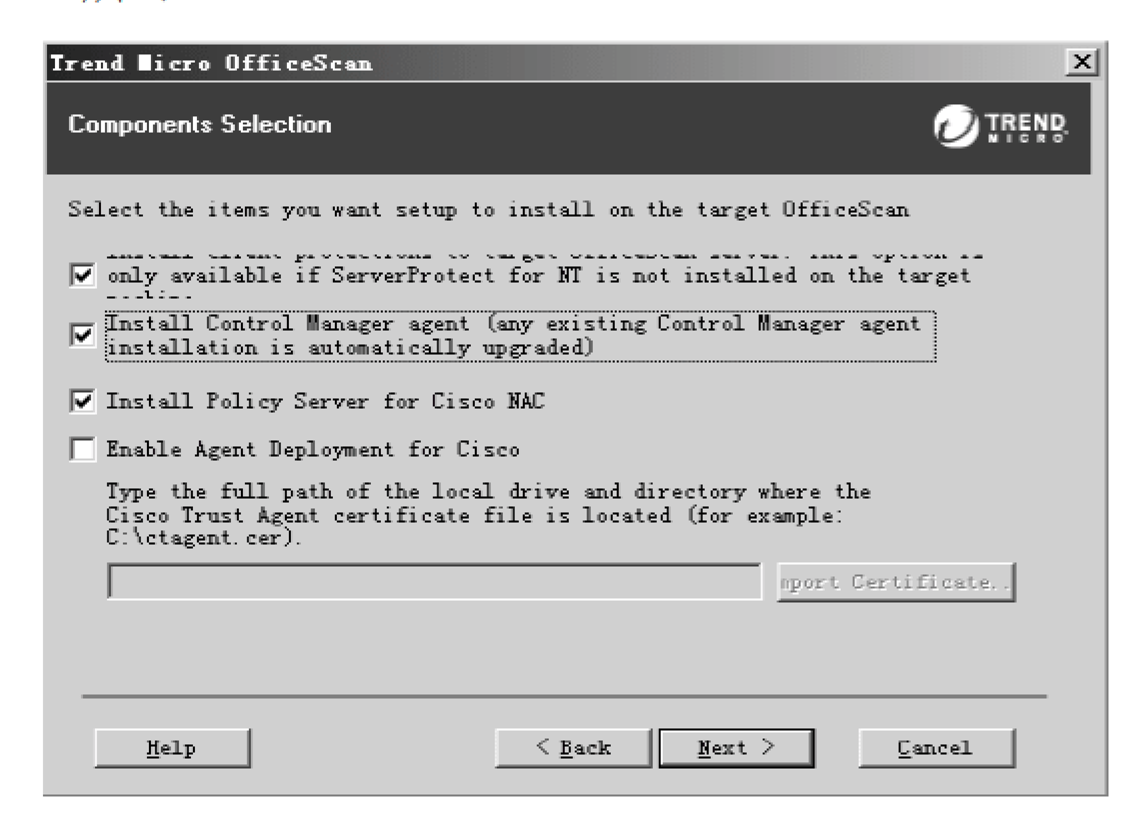


图 7-66　选中 Install Policy Server for Cisco NAC 复选框

❸ 在安装过程中，可以选择 Policy Server 的端口以及 Console 管理密码。在此，我们使用默认的端口配置(http: 8081，https:4344)，如图 7-67 所示。

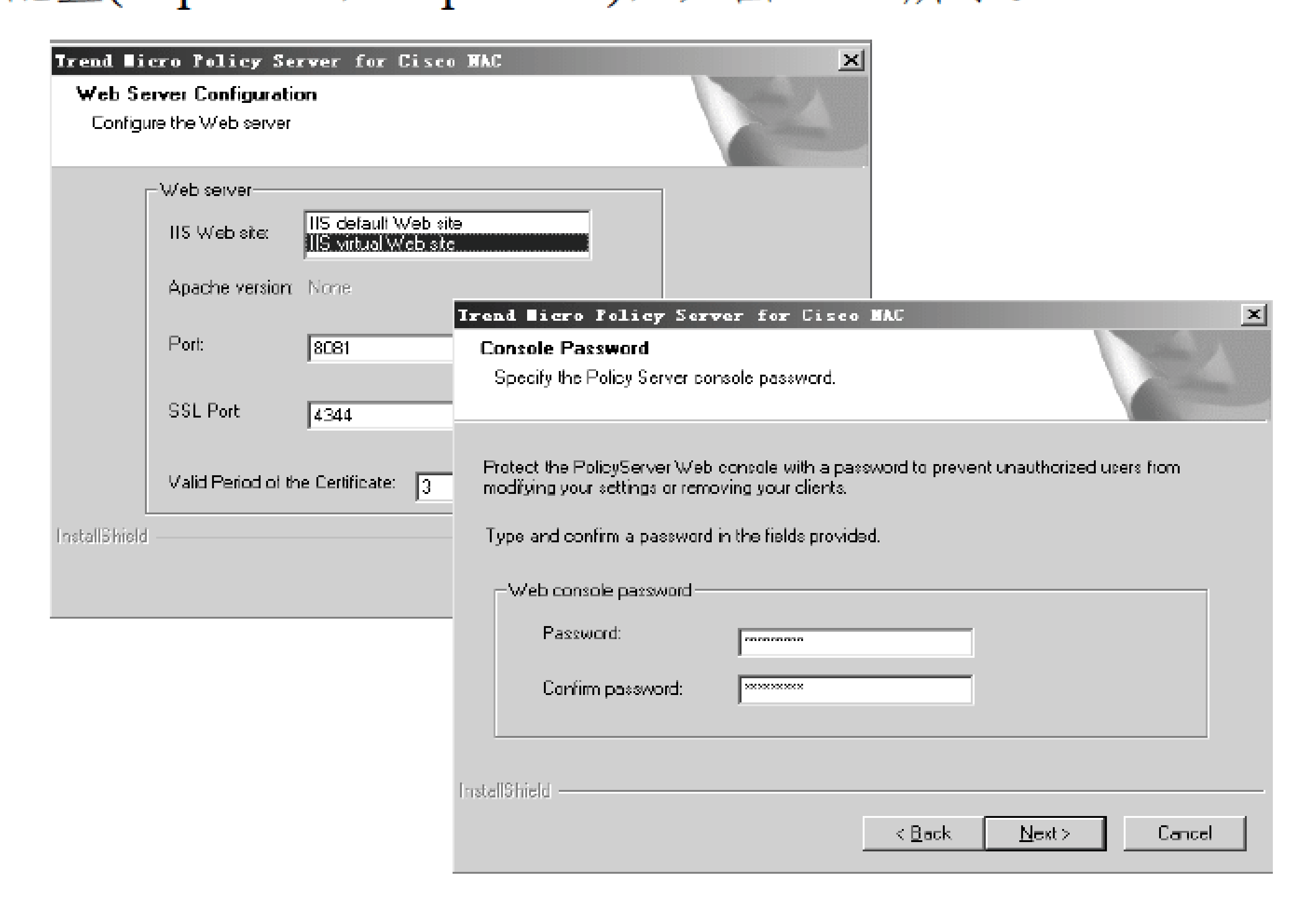


图 7-67　选择 Policy Server 端口以及管理密码

❹ 输入和先前 ACS 配置相关联的账号和密码，用于控制 Policy Server(策略服务器)，如图 7-68 所示。

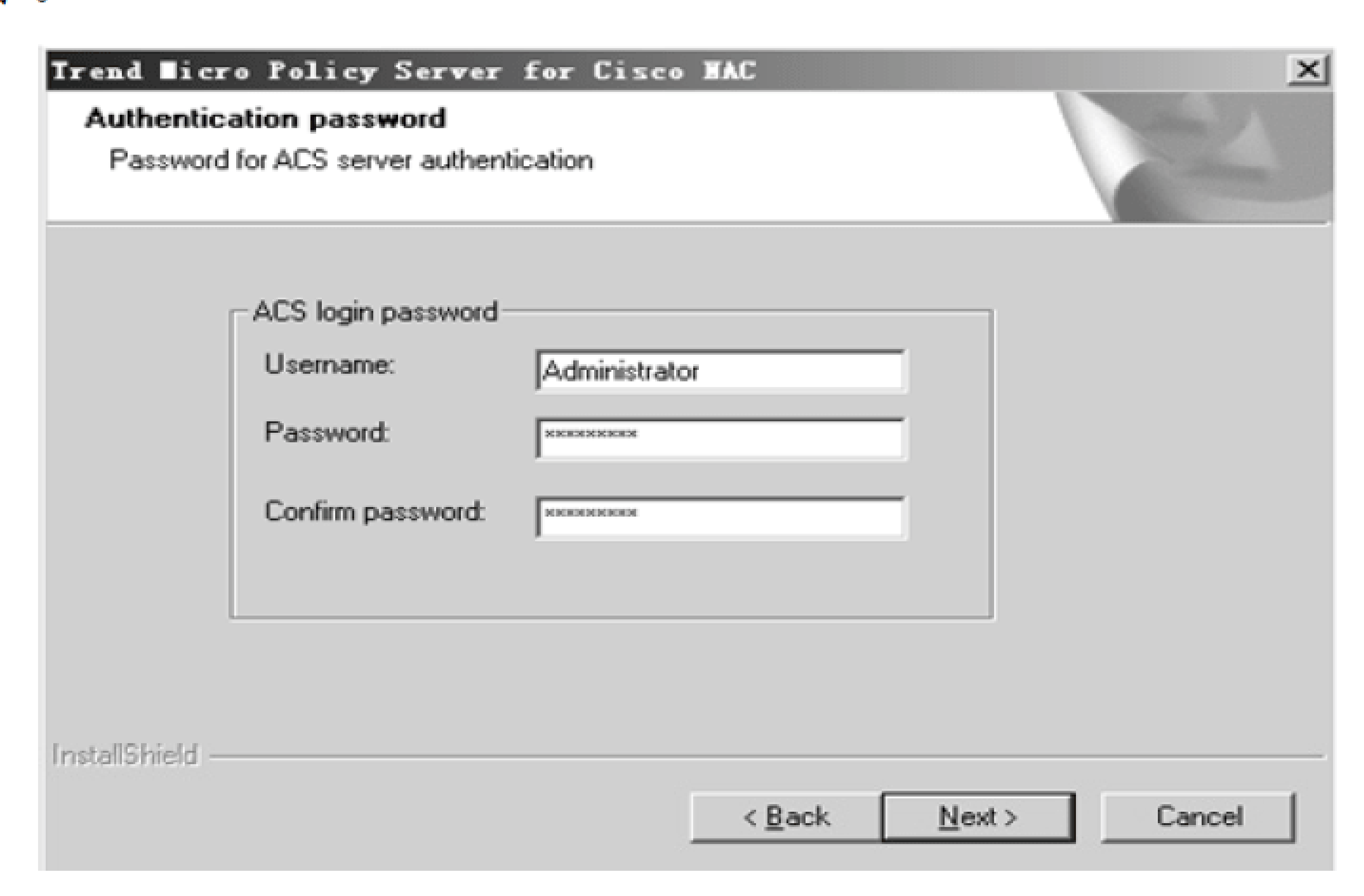


图 7-68　完成配置

❺ 通过“https://trendmicor-sv-ip:4344/”远程访问 Policy Server，输入管理员密码，进入配置界面，如图 7-69 所示。

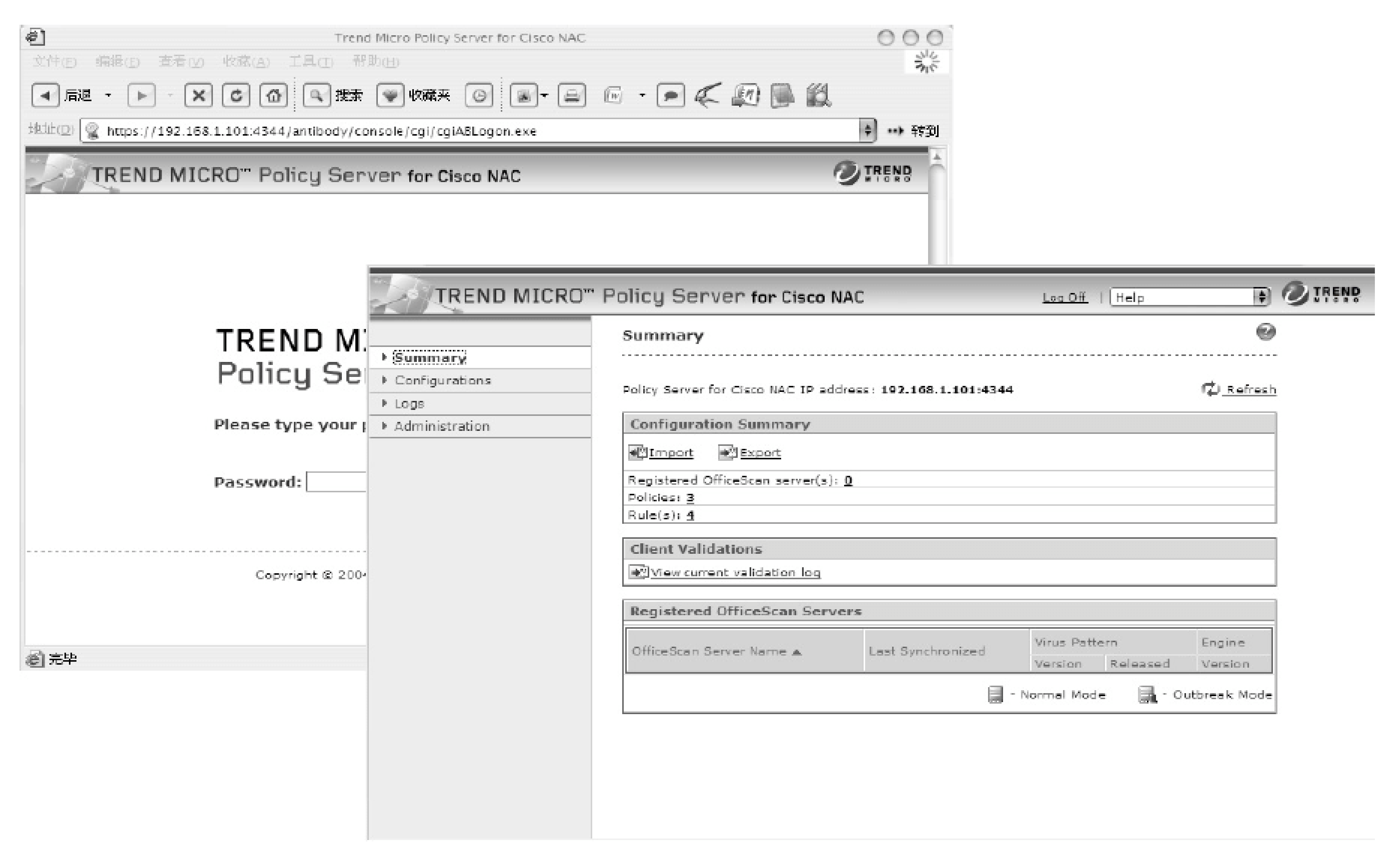


图 7-69　配置 TM Policy Server

❻ 依次选择 Configurations→Rules 命令配置各种规则。TM Policy Server 已经内置了 4 种规则，分别为：CheckUp、Healthy、Not Protected 和 Quarantine 配置策略。如果管理员需要定义新的规则，可以在这个页面添加，如图 7-70 所示。

❼ 配置完相应的规则后，可以依次选择 Configurations→Policy 命令来定义策略，并在其中可以自定义相应的消息，返回给 CTA，如图 7-71 所示。

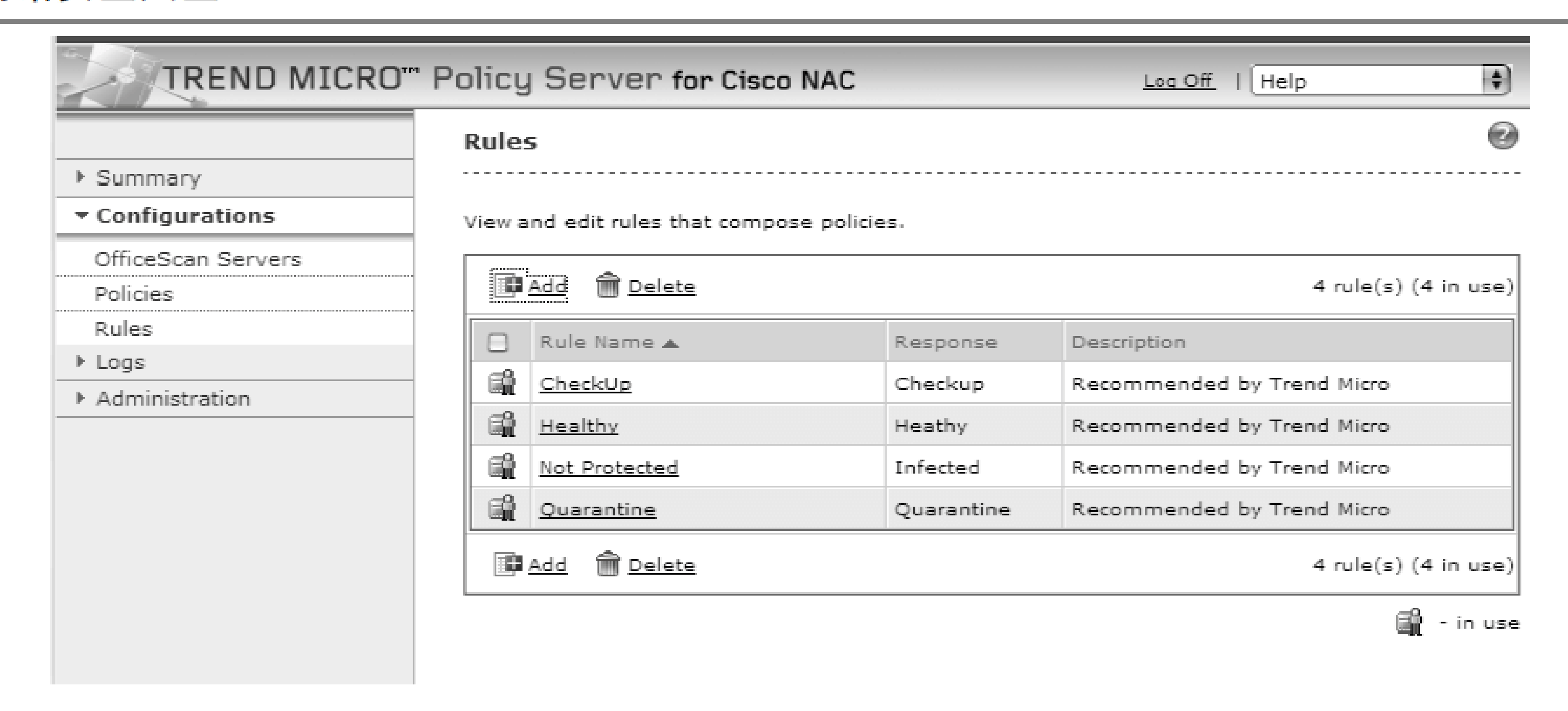


图 7-70　配置 TM Policy Server 规则

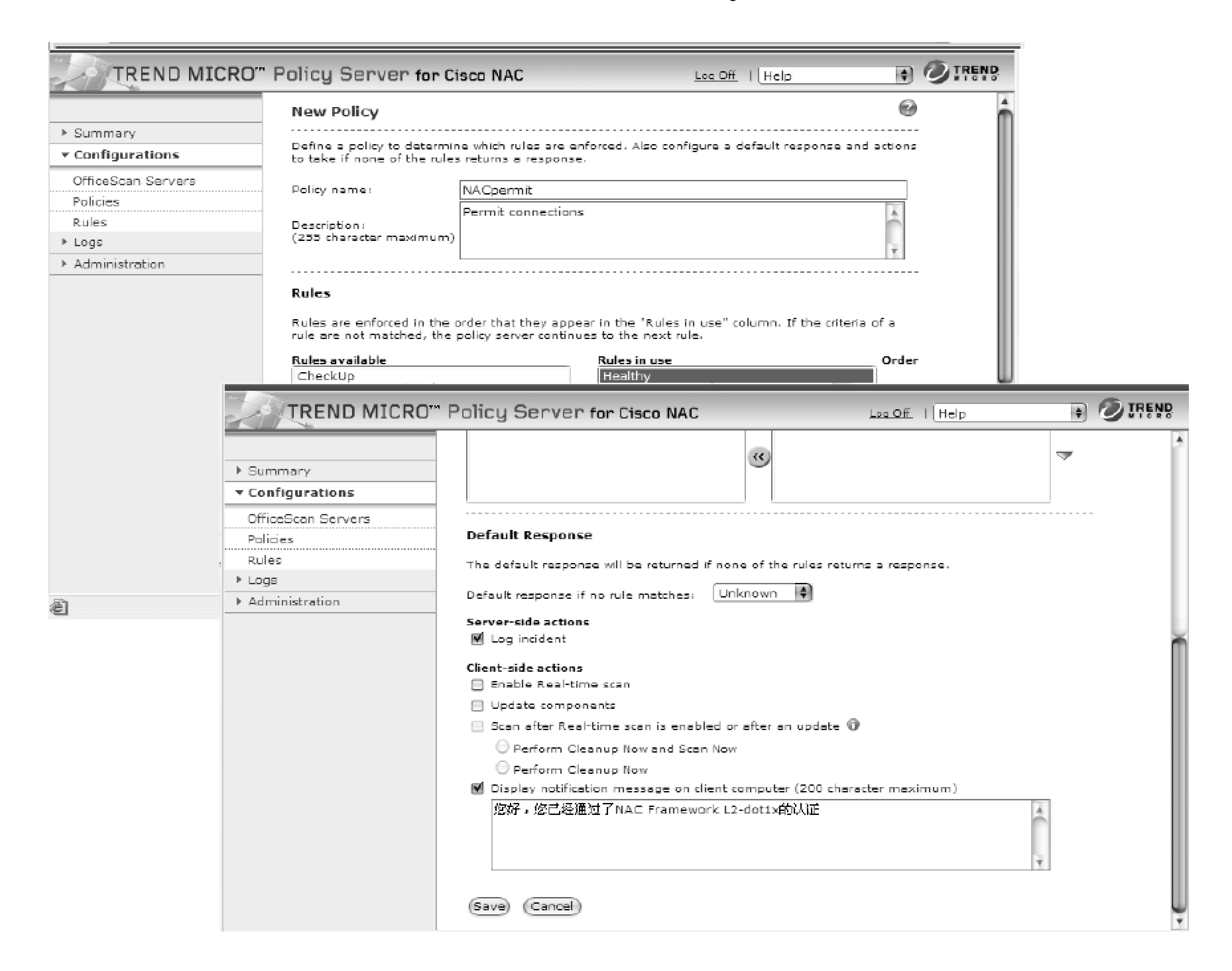


图 7-71　配置 TM Policy Server 策略

4. 安装 Cisco Trust Agent

上面已经介绍了 NAC Framework L2-dot1x 架构中相关服务器和交换机的配置方法，对于每一台客户机还需要安装和配置 Cisco Trust Agent。

❶ 在安装 Cisco Trust Agent 前，需要在 CTA 安装目录下建立一个名为 Certs 的目录，并将 ACS 的证书文件放在这个目录下，则 CTA 安装完成后将自动安装这个证书，如图 7-72 所示。



图 7-72　安装 Cisco Trust Agent

❷ 完成安装后重新启动计算机，当接入交换机时，系统将自动进行认证和状态确认的过程，如图 7-73 所示。

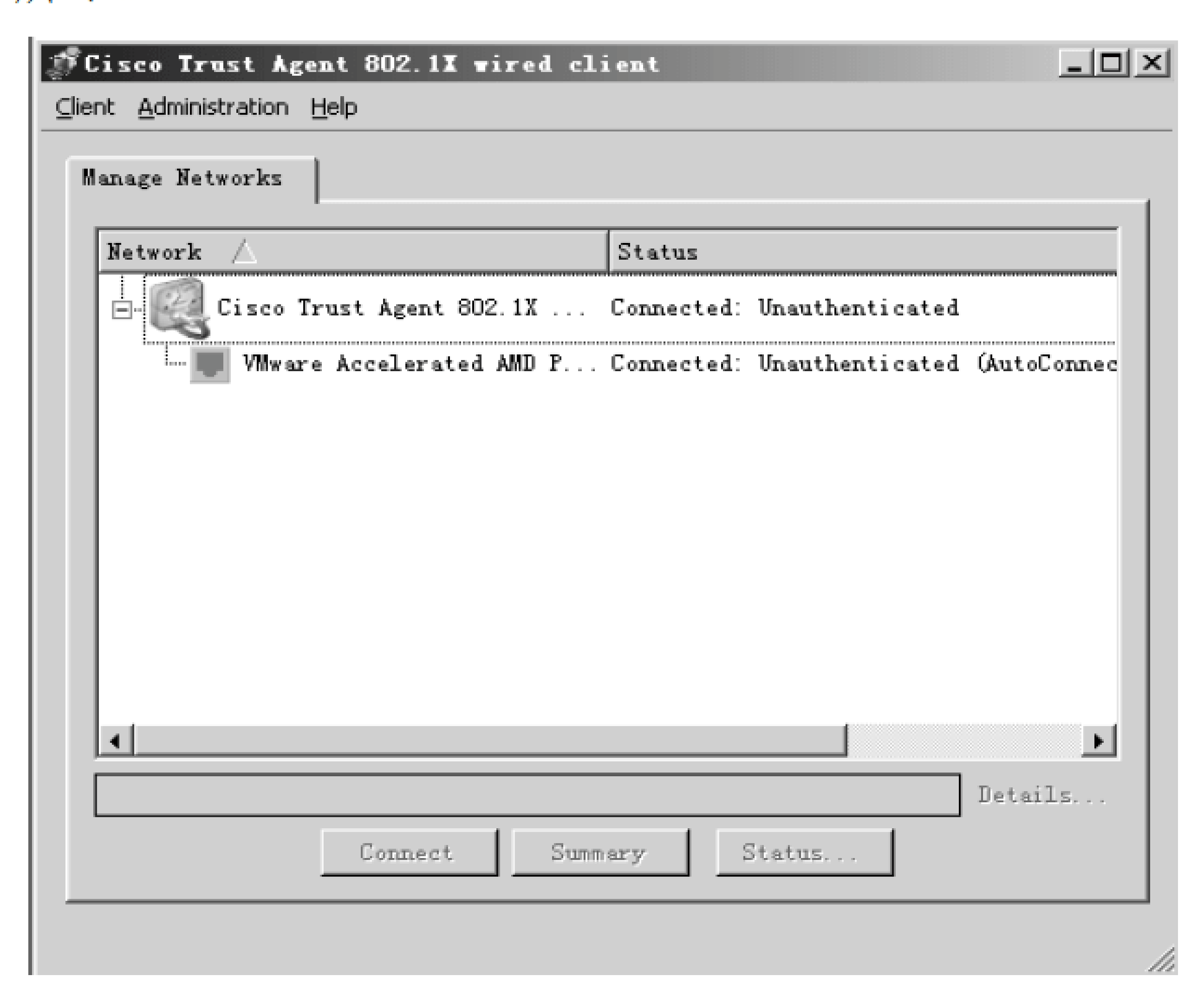


图 7-73　完成 NAC 认证

至此，我们完成了 NAC Framework L2-802.1x 的配置。

点评与拓展： Cisco NAC 是一个相对较为安全的网络准入认证方案。NAC Framework 是这个方案的第一阶段，它仅支持全网均为 Cisco 设备时的安全接入，但 NAC Framework 接入方案的价格相对低廉；而 NAC Appliance 则进一步加强了 NAC 的性能，支持多种设备，并且可以通过 in-band 的方式来应对接入交换机为非 Cisco 产品的解决方案。当然，终端安全除了网络准入控制外，Cisco 还支持基于 CSA 的终端保护方案，下一节我们将介绍这个技术。

7.4 终端保护机制

7.4.1 Cisco CSA 概述

Cisco 安全代理就是一种基于行为规则的终端防范技术，与传统的终端安全解决方案相比其不同之处在于：它可以在恶意行为发生之前发现并阻止它们，进而消除潜在的已知和未知的安全风险，防止其威胁到企业网络和应用的安全。因为 Cisco 安全代理采用的是分析行为而不是特征匹配的方法，因而这个解决方案能够以较低的运营成本提供强大的保护。当那些基于签名的防病毒软件、个人防火墙需要大量的签名库更新的时候，基于行为规则分析的 Cisco 安全代理却不需要那些费时费力的工作。Cisco 安全代理按照安全级别将行为分成三类。

1. 一般的恶意行为

这种行为一般都是在攻击周期的后期进行的破坏行为，例如未授权的对操作系统进行更改或文件删除。由于这类恶意行为总是不希望发生的，这个安全级别的部署将非常方便。这种类别相关的安全策略也一般不需要特别订制，默认状态即可

2. 总体安全策略相关行为

这些行为包括那些也许并不是明显恶意行为，但管理人员不希望其发生。例如网络管理员不希望用户通过那些即时通信软件(如 MSN Messenger、QQ、Yahoo Messenger 等)下载文件，因为这些文件无法经过公司的邮件防病毒服务器扫描。

3. 特定应用系统相关的行为

对于那些系统安全要求特别高的场合，Cisco 安全代理可以完全锁定整个特定应用。只有那些已知安全的行为才能被这个应用允许执行。通过强制限定这些合法、良好的行为，在这些合法行为之外的任何行为，无论是一个攻击还是简单的堆栈溢出错误，都可以被很有效地防范。其基本原理就是“任何没有明确被允许的将被禁止”。这种方法提供了最高的系统安全，但也需要更多的管理人员的调整。一般只限于某些重要的服务器。

7.4.2 Cisco CSA 架构及工作原理

CSA(Cisco Security Agent，Cisco 安全代理)由于具有同操作系统内核紧密结合的特点，所有对系统资源、配置、网络应用、文件读写等的呼叫都将被 Cisco 安全代理所截获，这种技术称为 INCORE(Intercept Correlate Rules Engine)技术。

比简单截获这些系统呼叫更重要的是，Cisco 安全代理将这些系统呼叫实现智能的关联。这些关联结果和对某个应用的行为规则的结论性理解形成了 Cisco 安全代理防范新的入侵的基础。

当一个应用程序需要访问某个系统资源时，它会产生一个操作系统呼叫到系统内核。

INCORE 会截取这些呼叫然后将这些呼叫同那些存储在中心服务器上的策略进行比较(这些策略也可以下载各个终端)。它会将这个特定的系统呼叫同该应用发起其他呼叫进行关联，然后来检测恶意的行为。如果呼叫请求没有违反任何的策略，将会提交内核运行；如果确实违法了策略，将会被阻止，一个相应的错误信息将会被传递回应用程序，然后一个警告将会产生并送往管理终端。

Cisco 安全代理策略是 IT 部门分配给每个服务器或工作站的行为规则的集合。这种以应用为中心的访问控制规则(不是基于用户或 ID)提供对需求资源的安全控制。Cisco 为企业提供能够容易被应用或模块化的订制策略部署工具。Cisco 安全代理能够为服务器迅速提供重要的入侵保护功能和分布式防火墙能力，这种解决方案也可以非常容易地被部署用作保护一些公共应用程序，例如 Microsoft SQL 服务器、Microsoft Office、即时通信软件、IIS Web 服务器等。这些策略能够被在最少配置的情况下迅速部署保护关键服务器和工作站。

Cisco 安全代理的管理中心采用代理-管理器(服务器)的架构(如图 7-74 所示)，当某个策略在管理服务器上创建或修改时会自动地分配到所有的代理终端上。管理员可以通过一个安全的 Web 页面进入管理图形界面，允许在企业内部任何地方来进行管理，避免使用那些不安全的远程访问方式。代理终端也会定时轮询服务器获得策略更新或是软件版本更新，或实时发送警告信息。所有的代理-管理服务器之间的通信都是加密的和使用标准协议。

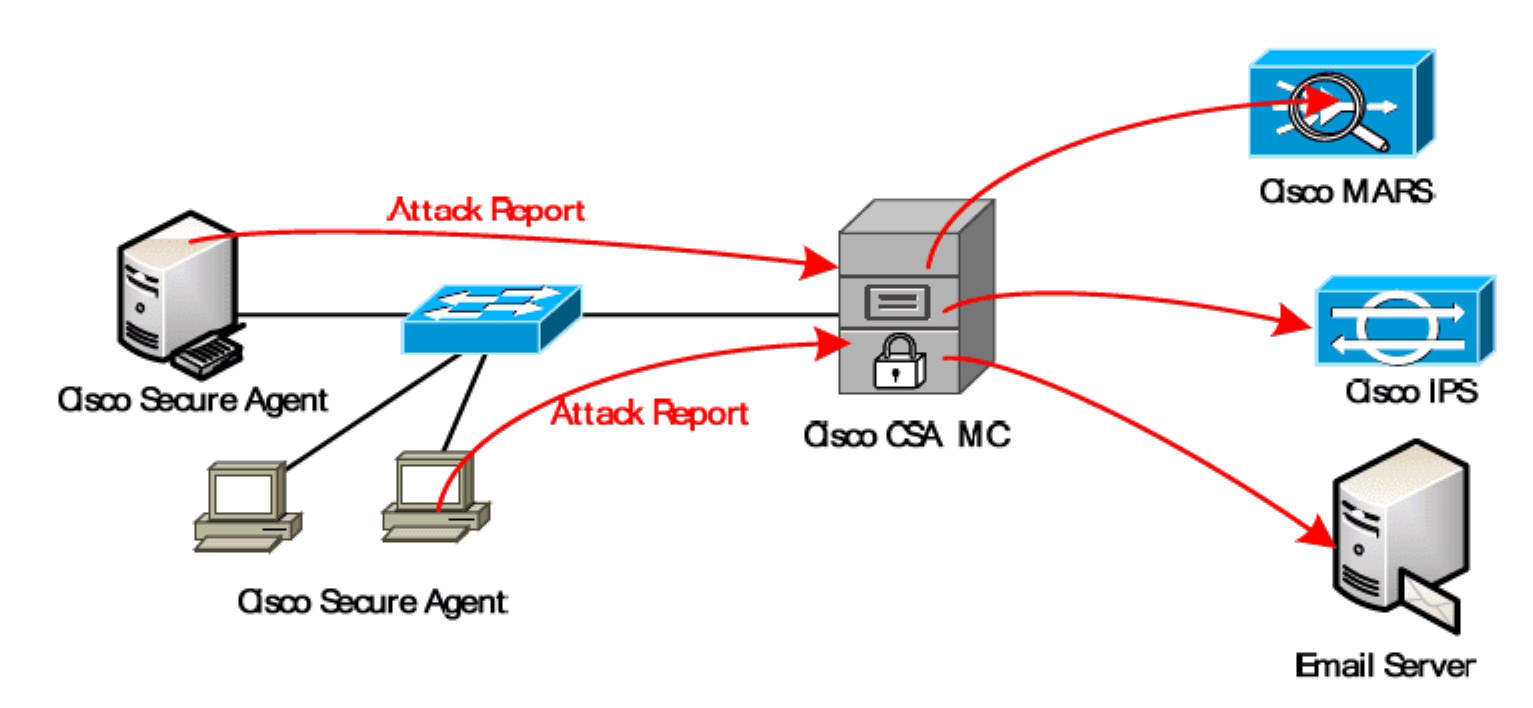


图 7-74　Cisco CSA 架构

CSA 服务器端称为 Cisco 安全代理管理中心(Cisco CSAMC，CiscoWorks Management Center for Cisco Security Agents)，当出现异常后，Cisco CSA MC 还会向 CS-MARS、Cisco IPS，以及电子邮件和 Web 等多种方式向外报告异常行为。同时，当管理员定义了相应的异常处理行为后，CSA MC 将主动把这些策略向下分发到 CSA，完成安全部署。

以 Nimda 病毒为例，Nimda 是一种传播非常迅速的病毒，它能够通过电子邮件的附件、浏览受感染的网站的用户，以及利用存在漏洞的 Microsoft IIS Web 服务器在企业中传播。传统的做法是采用路由器或交换机上基于 NBAR(基于网络的应用识别)的过滤方式，其配置如下。

```
ip cef
!
class-map match-all DENY-ATTACK
match protocol http url "*.ida*"
match protocol http url "*cmd.exe*"
```

```
match protocol http url "*root.exe*"
match protocol http url "*readme.eml*"
match protocol http url "*readme.exe*"
!
policy-map denynimda class DENY-ATTACK drop
interface FastEthernet 1/0
ip address 10.0.0.1 255.255.255.252
service-policy input denynimda
```

然而，这种阻止 Nimda 进一步扩散的方式与 Microsoft 公司已经发布了针对 IIS 服务器漏洞及 Internet Explorer 补丁一样属于被动防御结构，在受到攻击后仍然有大量的设备被感染。CSA 中的默认 IIS 和桌面策略可以防止企业受到 Nimda 的攻击。在遭遇 Nimda 病毒时，CSA CM 可以发送策略给 CSA 阻止针对 IIS 服务器的缓存溢出攻击，防止它在网络中传播。CSA 的默认桌面策略也可以禁止下载和调用木马程序，例如 readme.exe 等，在 Nimda 试图通过 Outlook 或者 Web 浏览器感染一个企业时，可以有效地防止 Nimda 对企业造成损失和在企业中蔓延。

7.4.3 安装 Cisco CSA MC

Cisco CSA MC 是整个 CSA 体系中最重要的部分。它是 CSA 的管理器，用于策略的创建、修改以及分配。这种通常 CSA MC 可以支持三种安装模式。

- ✧ 安装 CSA MC 和数据库在同一台服务器上(安装 CSA MC 时选择 Local Database 按钮)：这种模式的数据库使用 Microsoft SQL Server 2005 Express Edition，仅支持少量客户端；当然，用户可以安装 SQL Server 2005 支持 5000 用户的环境。
- ✧ 安装 CSA MC 在一台服务器上，数据库安装到远程的另一台设备上 (安装 CSA MC 时选择 Remote Database 按钮)：这种模式的数据库和 MC 分离，进一步提高了安全性和性能。需要注意的是，两台机器需要用 NTP 同步时钟，并且同样支持 5000 用户的环境。
- ✧ 将两个 CSA MC 分别安装到两台服务器上，数据库安装到远程的另一台设备上，两个 CSA MC 使用同一个数据库。(安装 CSA MC 时选择 Remote Database 按钮)：这种模式是 Cisco 推荐给较大规模企业网络部署的模式，可以支持 100 000 用户，并且其中一个 MC 用于客户端注册和策略分法，另一个 MC 用于策略编辑和配置。

下面介绍的是基于 Windows Server 2003 R2 的平台上安装 CSA MC 的过程。

❶ 双击 CSA MC 安装程序，在欢迎界面中单击 Next 按钮，同意协议后，再次单击 Next 按钮，如图 7-75 所示。

❷ 在数据库选择对话框中，如果为上述第一种安装模式，采用单台主机安装 CSA MC，则选择 Local Database，如果为后两种安装模式，则选择 Remote Database ，如图 7-76 所示。

❸ 选择 Local Database 安装方式后，如果系统没有安装 Microsoft SQL Server 2005，则会弹出对话框提示安装 Microsoft SQL Server 2005 Express Edition，单击 Yes 按钮。



图 7-75　安装 Cisco CSA MC

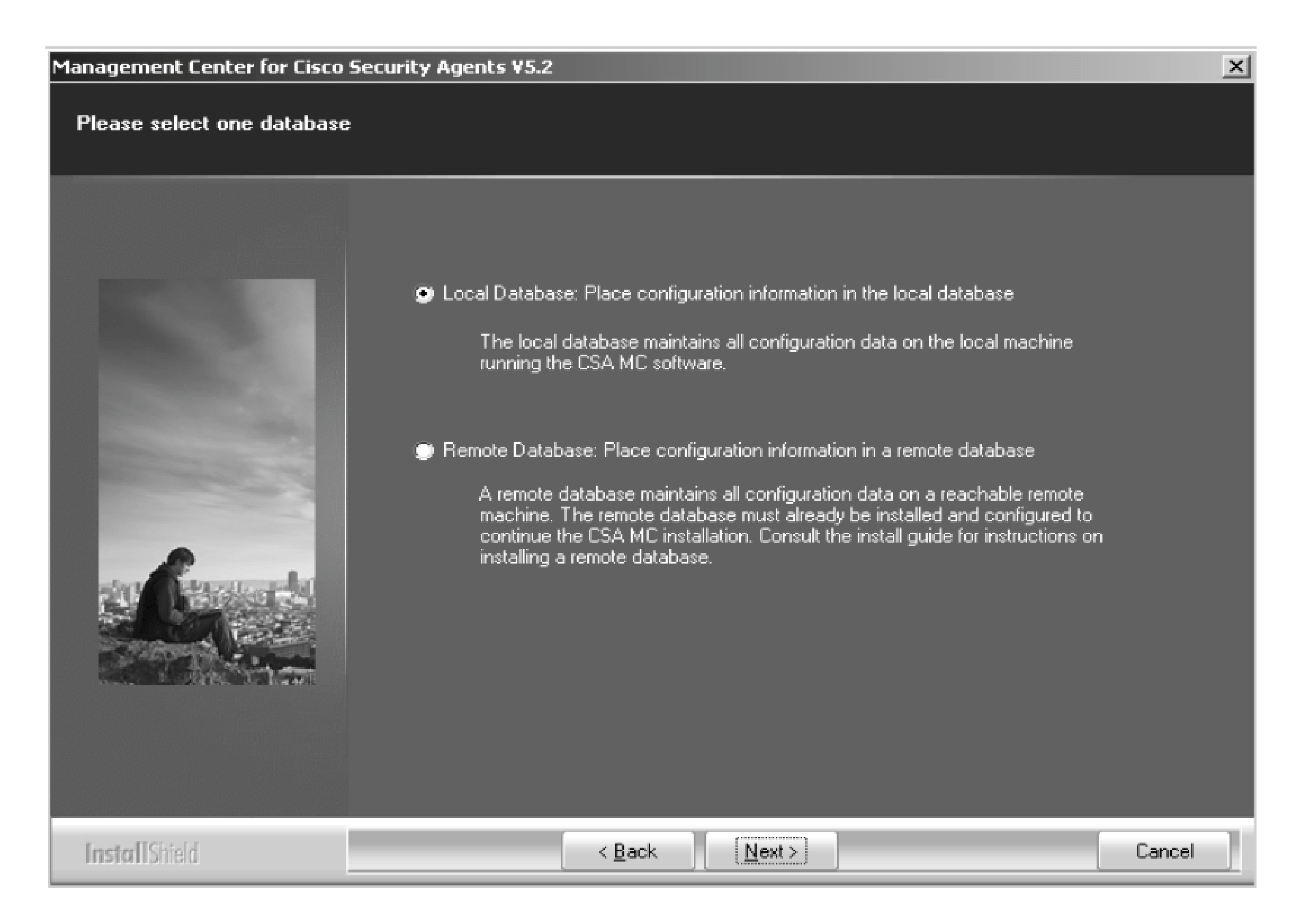


图 7-76　选择 Cisco CSA MC 数据库类型

❹ 在选择安装目录的对话框，选用默认设置并单击 Next 按钮，系统会提示输入管理员名称和密码，单击 Next 按钮，如图 7-77 所示。



图 7-77　配置 Cisco CSA MC 管理账户

❺ 开始安装系统，并在安装完成后自动重新启动计算机，如图 7-78 所示。



图 7-78　开始安装 Cisco CSA MC

❻ 重新启动后，在浏览器中输入“https://CSAMC-ip/csamc52/webadmin?page=login”，可以以 Web 方式访问 MC ，如图 7-79 所示。

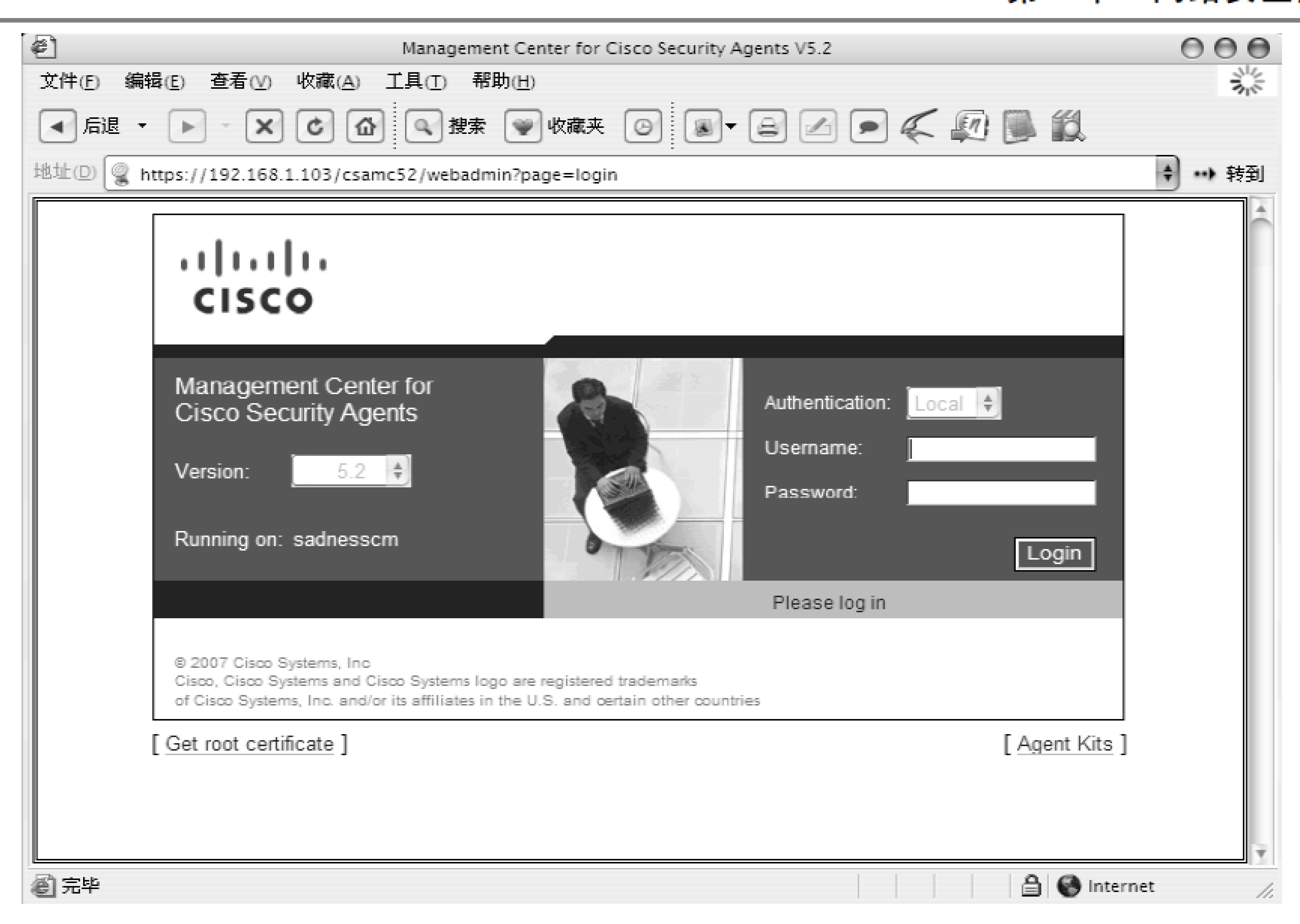


图 7-79　以 Web 方式登录 Cisco CSA MC

❼ 输入用户名和密码后即可登录 CSA MC。在管理界面菜单中包含了事件、系统、配置、分析、维护、报告、查找和帮助 8 大功能模块，如图 7-80 所示。

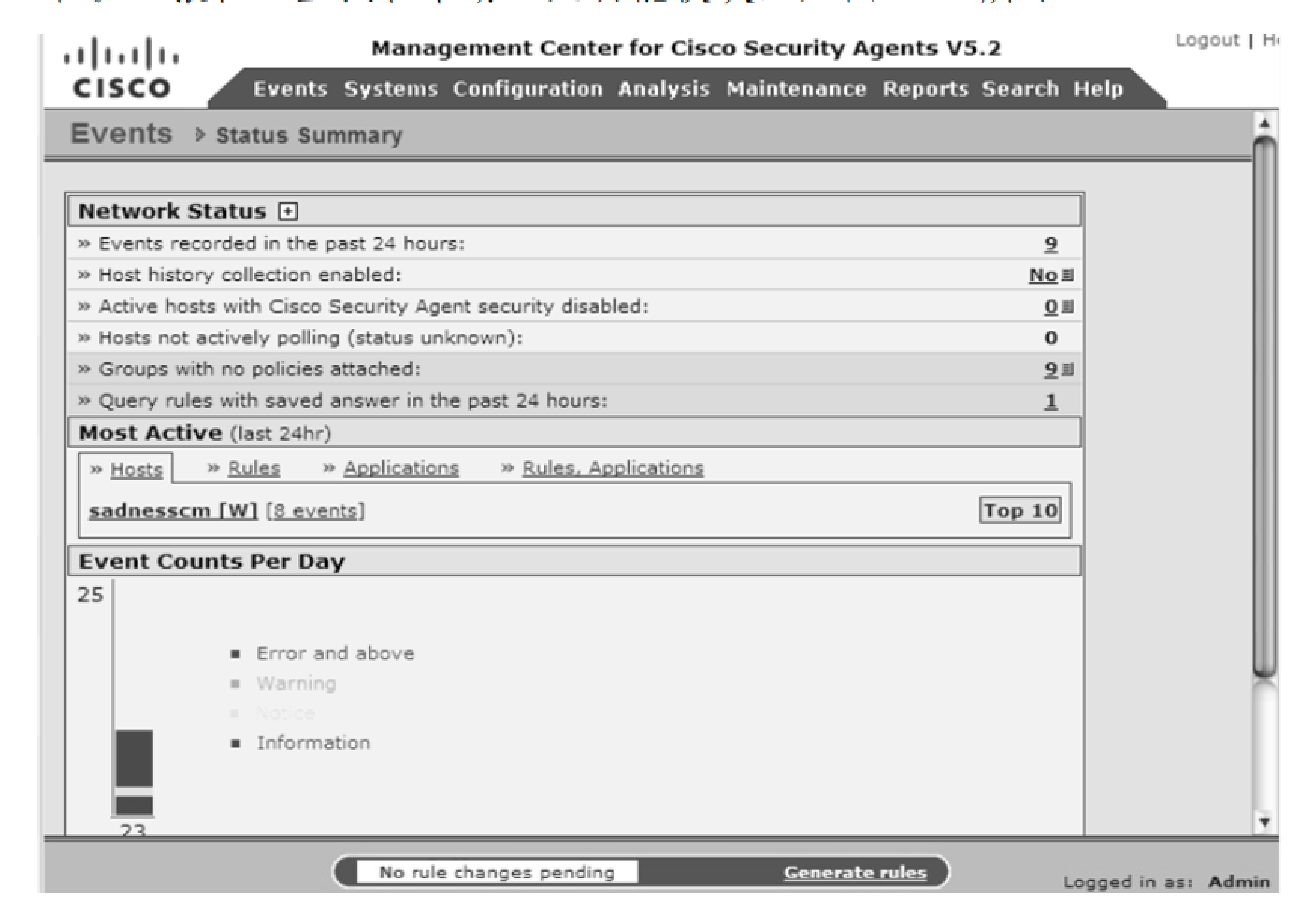


图 7-80　登录 Cisco CSA MC

❽ 加载注册文件。选择 Maintenance→License Information 命令，将打开 Cisco 发给用户的 License 邮件，将附件中的.lic 文件另存到硬盘，并单击 CSA MC 中的【浏览】按钮，找到该文件，单击 Upload 按钮即可导入 License ，如图 7-81 所示。

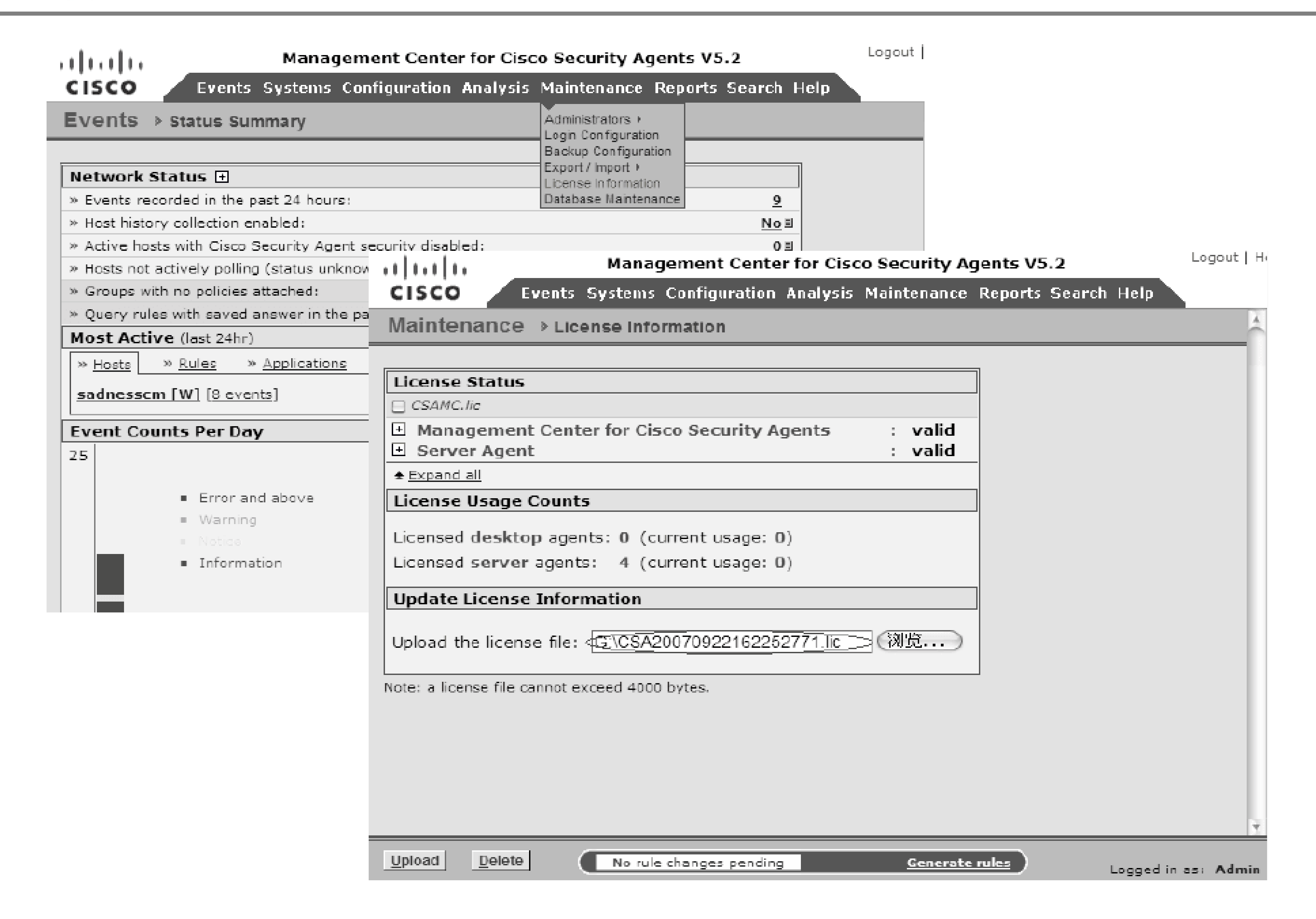


图 7-81　导入 License

7.4.4　配置 Cisco CSA MC

Cisco CSA MC 内含预配置的组件来处理代理策略，它包括如下三个部分。

✧ 组(Group)：分配安全策略的主机的集合，(这里包括预置的 Servers-All Types、Desktops-All Types 和 Serves-Apache Web Servers 等组项)，并且一个主机根据功能划分可以成为多个组的成员。

✧ 策略(Policy)：附属于一个或多个组，一个策略是具有相似目的或互相依赖完成整个工作任务的规则模块的集合。

✧ 规则(Rule)：附属于一个或多个 Policy，它是一个用于实现一个目标规划的集合。

通过这三者的相互关联，形成了一个完善的基于行为的策略体系，并且主机组能够减少管理大量主机代理工具的负担。网络中的全部主机，包括该域中的移动主机，只有安装和配置了管理中心赋予策略的安全代理工具的主机，才能够注册到管理中心并接受安全防护管理。

Cisco CSA MC 全部基于 Web 方式配置，可以用如下 URL 登录到管理界面。

```
http://<Cisco CSA MC-ip地址>/csamc52/webadmin?page=login
```

❶ 添加组。依次单击 System→Groups 命令，可以看到系统已经为 Linux、Solaris 和 Windows 三种系统定义了很多默认组，用户可以单击左下角的 New 按钮添加组。添加组时，首先系统会让用户选择可支持的平台，选择后在新的窗口中就可以定义组名、详细描述以及导入配置间隔(Polling Interval)等参数。单击 Save 按钮保存配置，如图 7-82 所示。

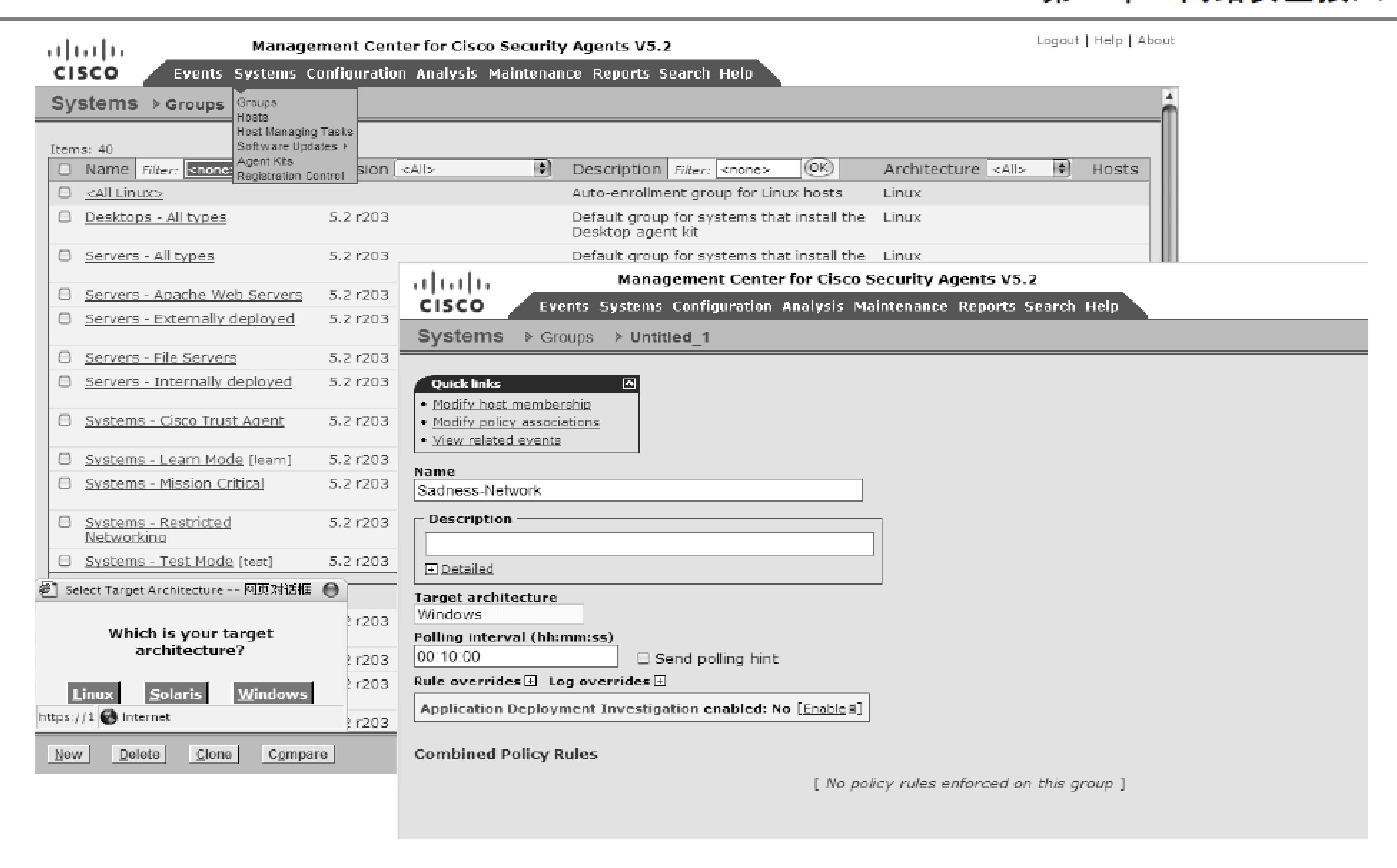


图 7-82　添加组 CSA MC 中的 Group

❷ 配置策略。依次单击 Configuration→Polices 命令，如图 7-83 所示。

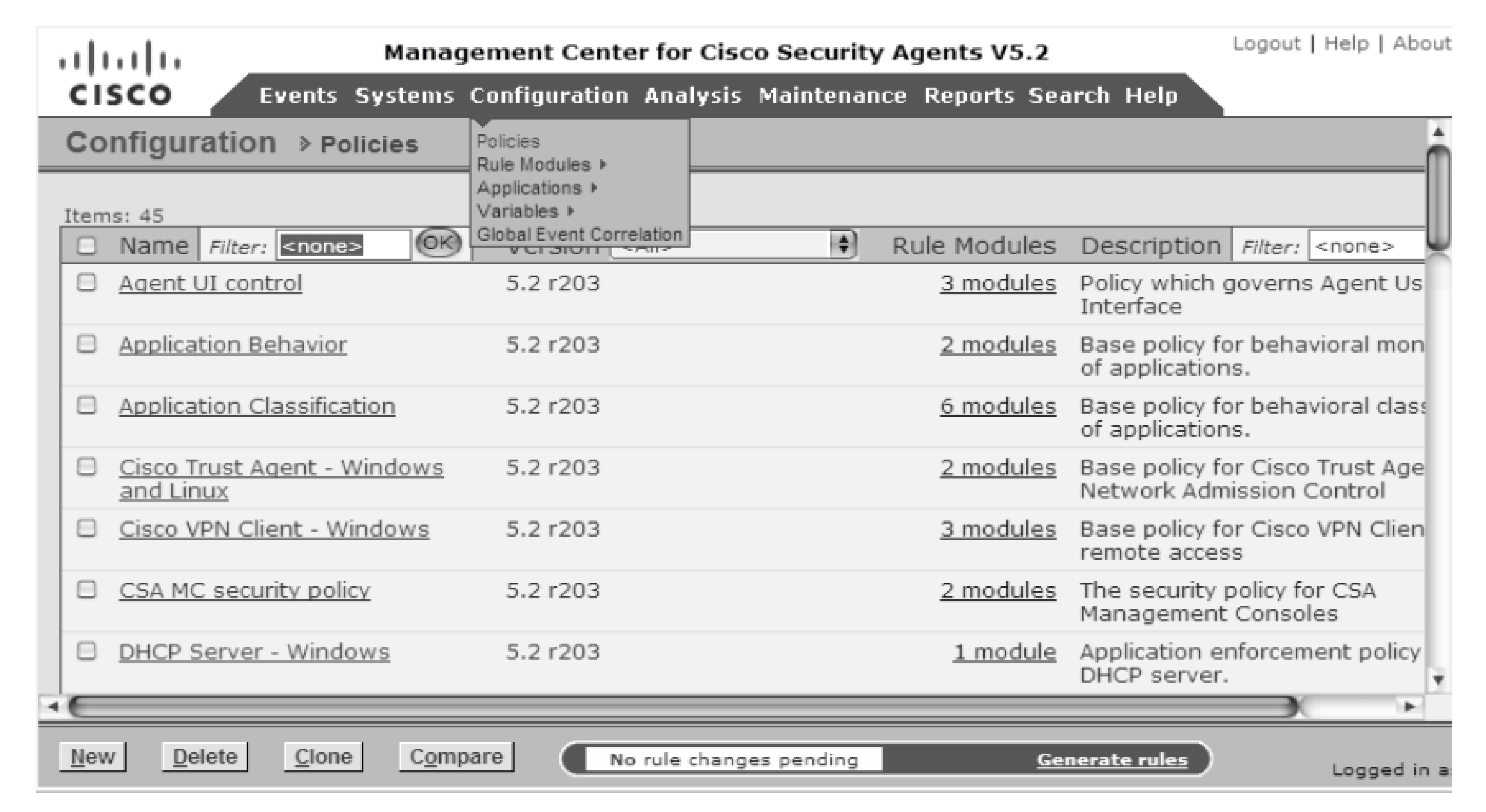


图 7-83　配置 CSA MC 策略

❸ 在策略配置页中，配置策略的名称、要应用到的目的系统等，如图 7-84 所示。

❹ 配置规则模式。依次单击 Configuration→Rule Module 命令，在子菜单中可以选择配置 Linux/Window 或者 Solaris 的规则，单击 New 按钮可以创建新规则组；并且在顶部可以单击 Modify Rules 进入规则配置模式，单击 Add Rule 按钮配置不同的规则，如图 7-85 所示。

❺ 将 CSA MC Policy 与 Group 和 Rule Module 进行关联。依次单击 Configuration→Policy 命令，选择相应的 Group 以及 Rule Module 进行关联，如图 7-86 所示。

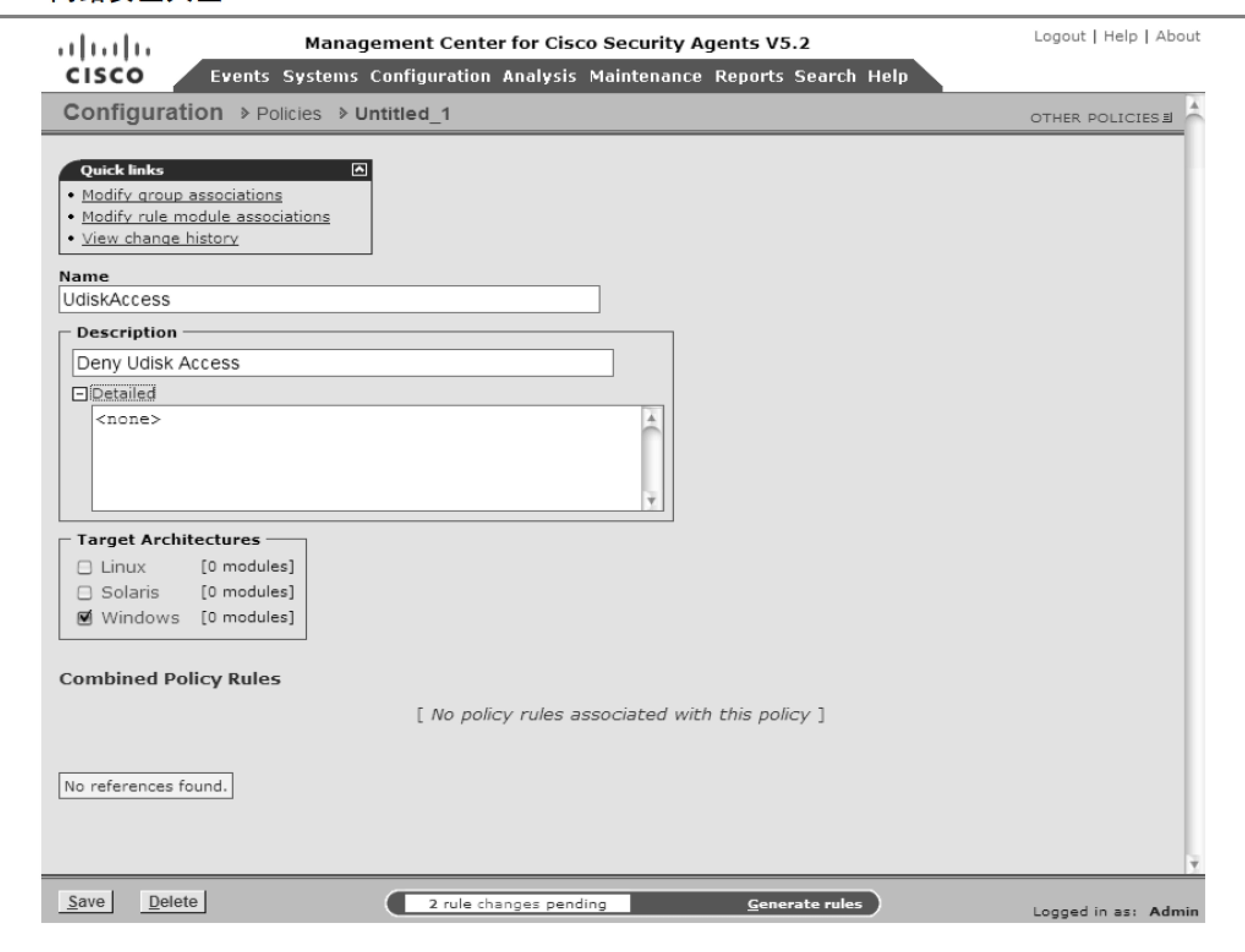


图 7-84 配置 CSA MC 策略

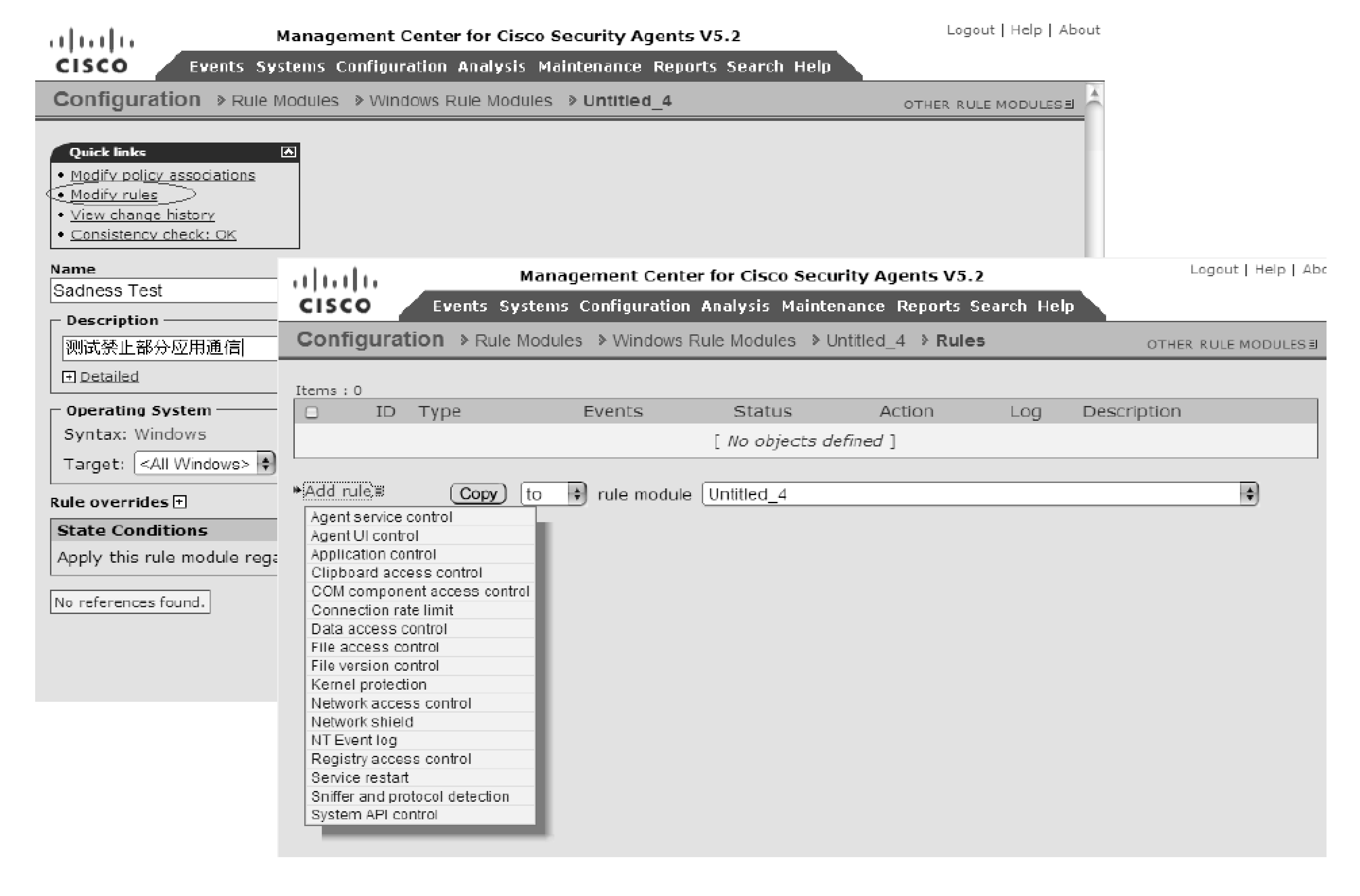


图 7-85 配置规划模式

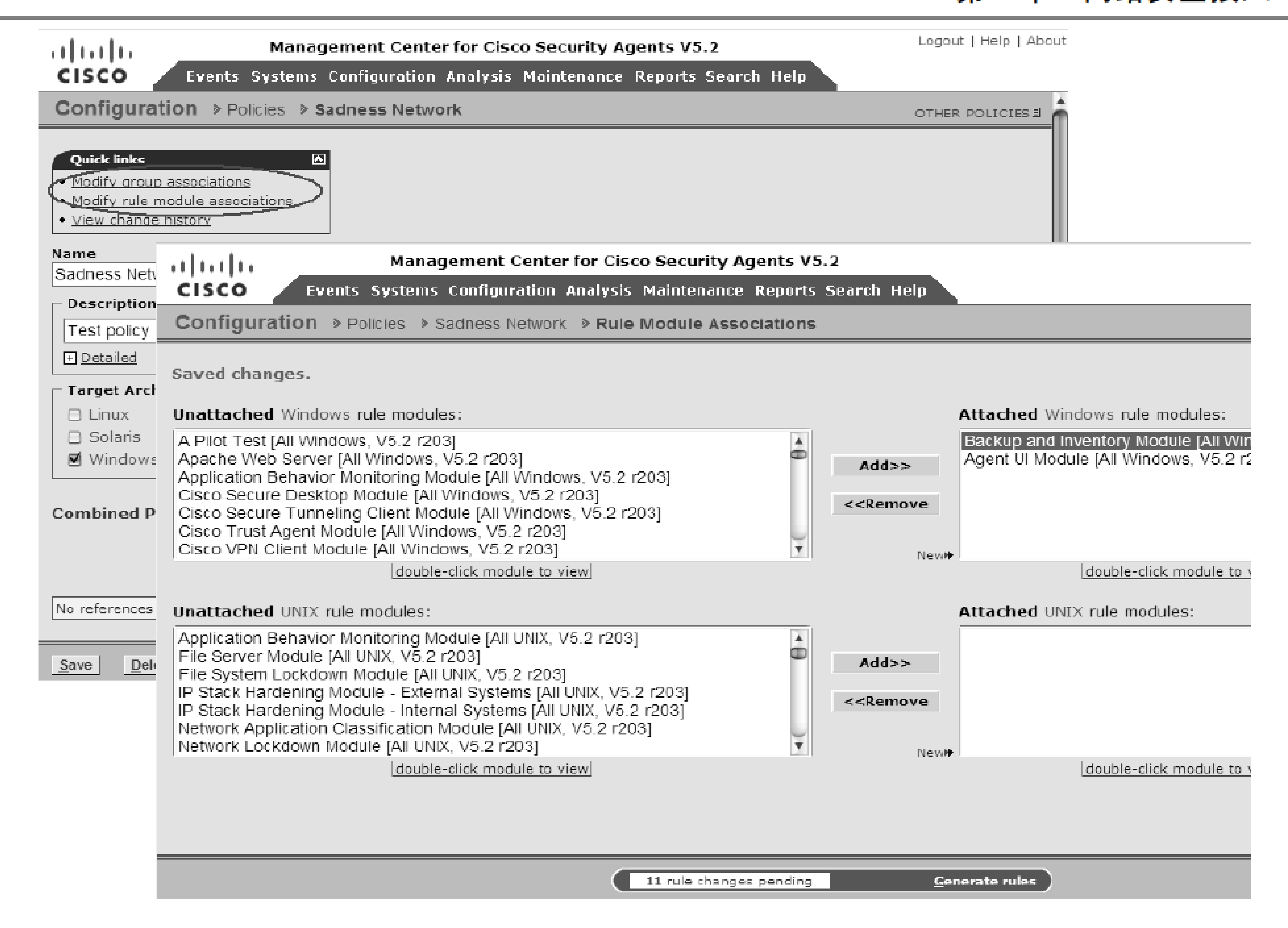


图 7-86　将 CSA MC Policy 与 Group 和 Rule Module 关联

❻ 创建客户 Host 需要下载的代理包。依次单击 Systems→Agent Kits 命令，选择安装方式为强制安装或静默安装等。完成配置后单击 Make kit 按钮，如图 7-87 所示。

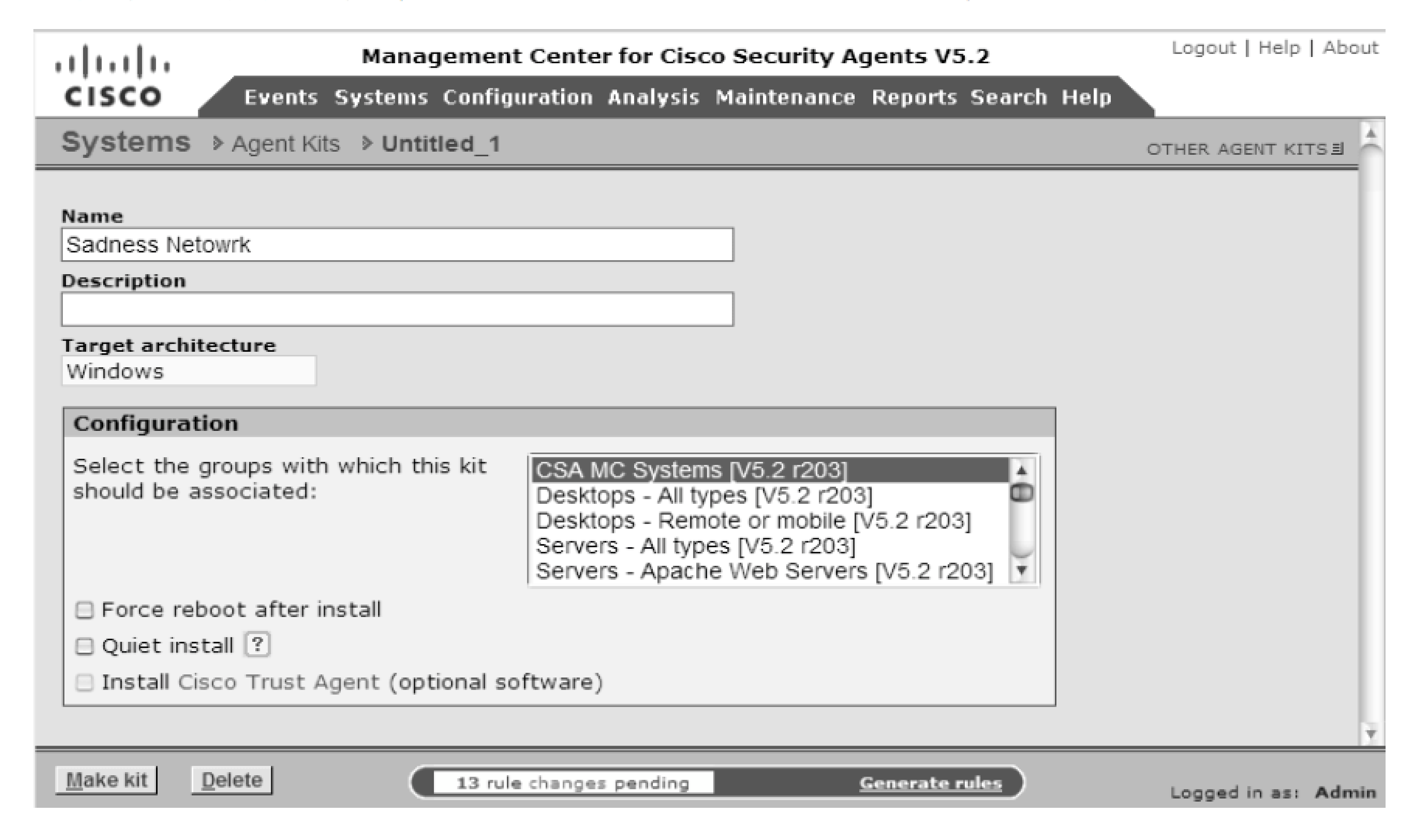


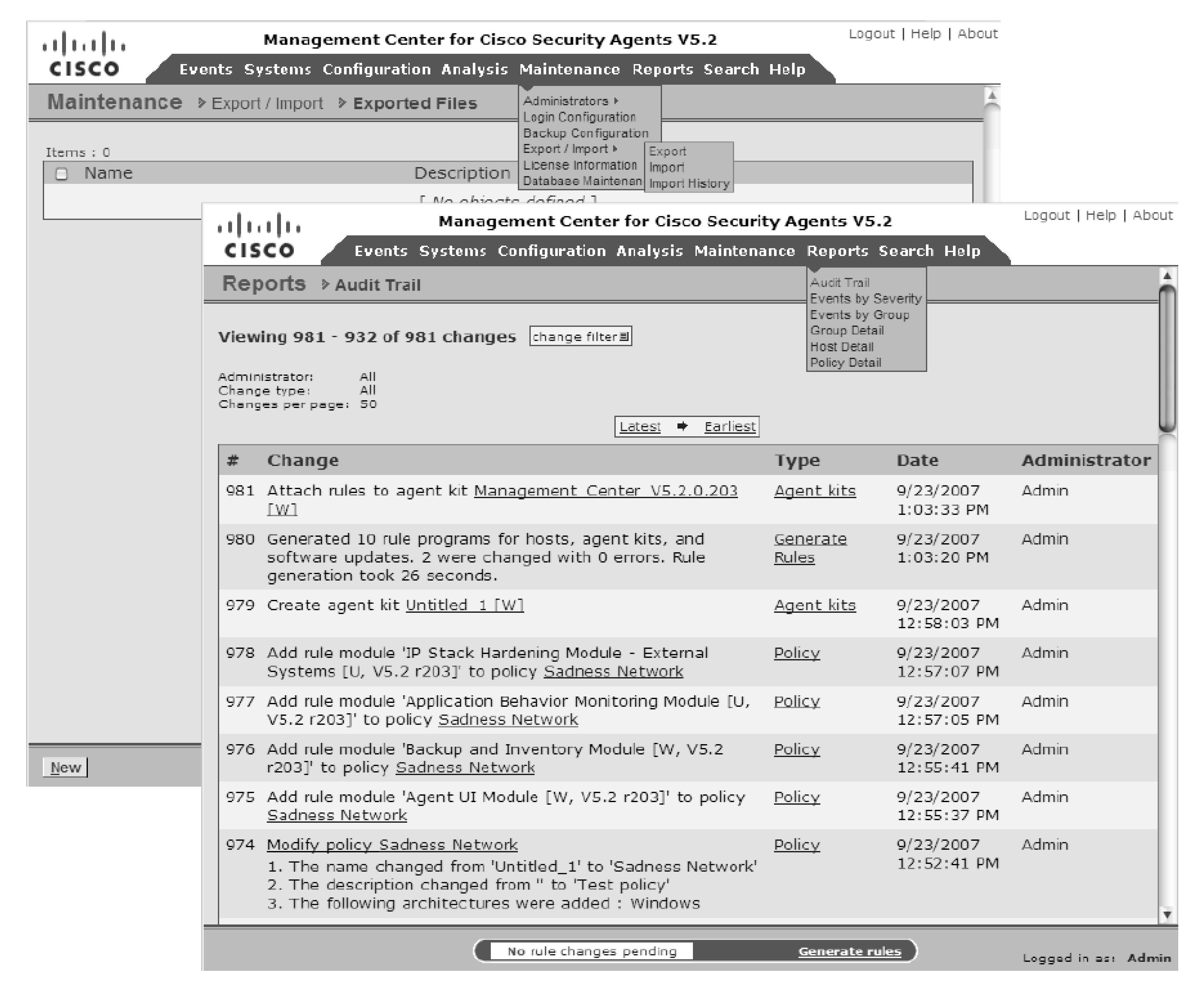
图 7-87　配置 Agent Kits

❼ 完成所有的配置后，单击 Generate Rules 按钮让 MC 完成所有规则的配置和发布，如图 7-88 所示。



图 7-88　完成配置和发布

❽ 导出、导入及审计配置文件。依次单击 Maintenance→Export/Import 命令，将配置文件进行导入和导出操作。对于所有 Cisco CSA MC 的配置行为，可以依次单击 Reports→Audit Trail 命令来查看，如图 7-89 所示。



#	Change	Type	Date	Administrator
981	Attach rules to agent kit Management Center V5.2.0.203 [W]	Agent kits	9/23/2007 1:03:33 PM	Admin
980	Generated 10 rule programs for hosts, agent kits, and software updates. 2 were changed with 0 errors. Rule generation took 26 seconds.	Generate Rules	9/23/2007 1:03:20 PM	Admin
979	Create agent kit Untitled_1 [W]	Agent kits	9/23/2007 12:58:03 PM	Admin
978	Add rule module 'IP Stack Hardening Module - External Systems [U, V5.2 r203]' to policy Sadness Network	Policy	9/23/2007 12:57:07 PM	Admin
977	Add rule module 'Application Behavior Monitoring Module [U, V5.2 r203]' to policy Sadness Network	Policy	9/23/2007 12:57:05 PM	Admin
976	Add rule module 'Backup and Inventory Module [W, V5.2 r203]' to policy Sadness Network	Policy	9/23/2007 12:55:41 PM	Admin
975	Add rule module 'Agent UI Module [W, V5.2 r203]' to policy Sadness Network	Policy	9/23/2007 12:55:37 PM	Admin
974	Modify policy Sadness Network 1. The name changed from 'Untitled_1' to 'Sadness Network' 2. The description changed from '' to 'Test policy' 3. The following architectures were added : Windows	Policy	9/23/2007 12:52:41 PM	Admin

图 7-89　导出、导入及审计配置文件

7.4.5　配置 Cisco CSA 客户端

Cisco CSA 服务器端安装与配置完成后，就可以配置 Cisco CSA 客户端了，下面简要地介绍一下其配置过程。

❶ 在客户端主机上，通过浏览器访问 “http://<Cisco CSA MC ip addr>/csamc52/kits”，选择 Test_Mode_Desktop_v5.2.0.203 链接下载 CSA 软件并进行安装。完成安装后，系统会自动重新启动，如图 7-90 所示。

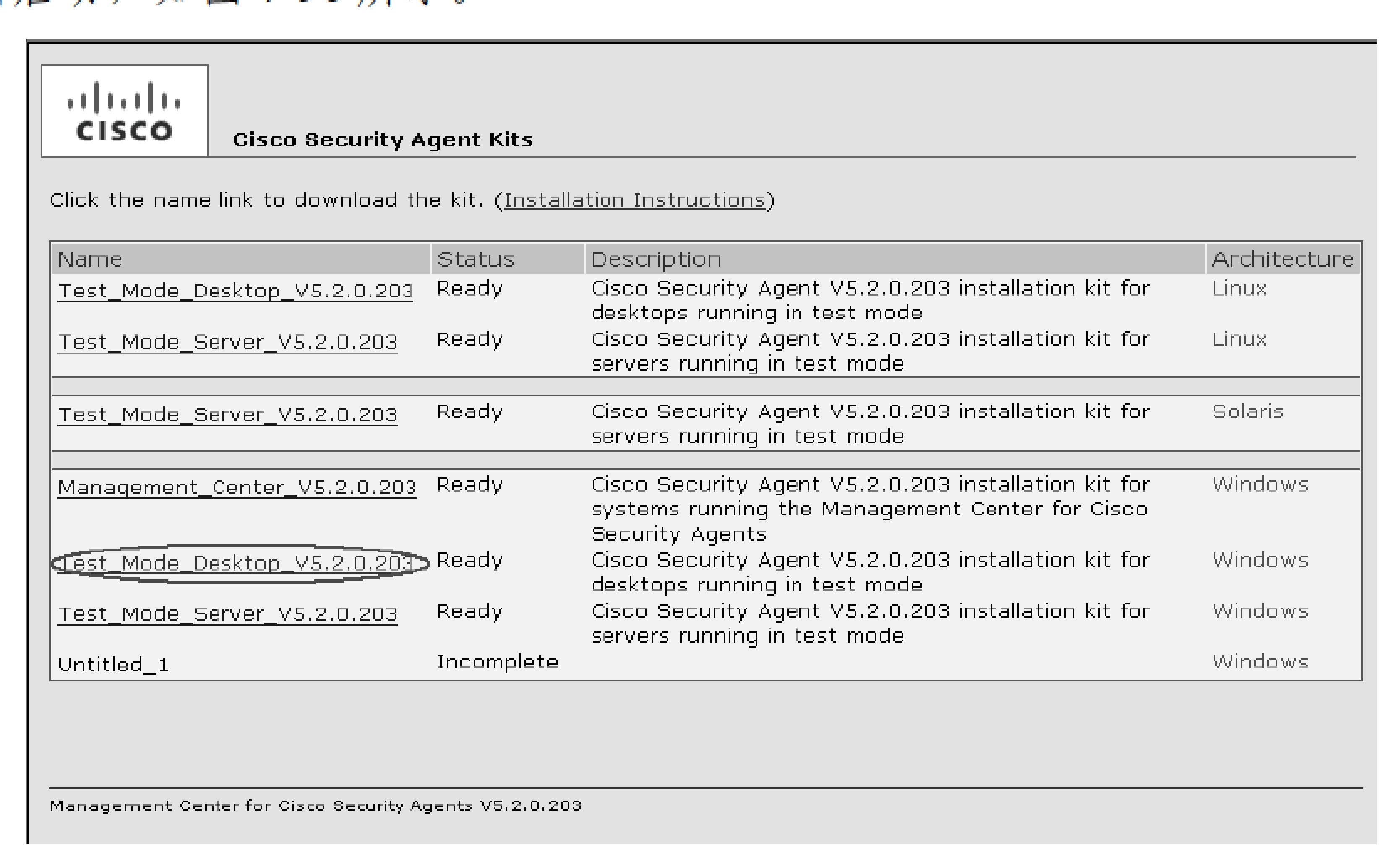


图 7-90　下载 CSA 客户端

❷ 安装完成后，可以通过 CSA 设置安全等级，以及轮询管理服务器的策略，如图 7-91 所示。

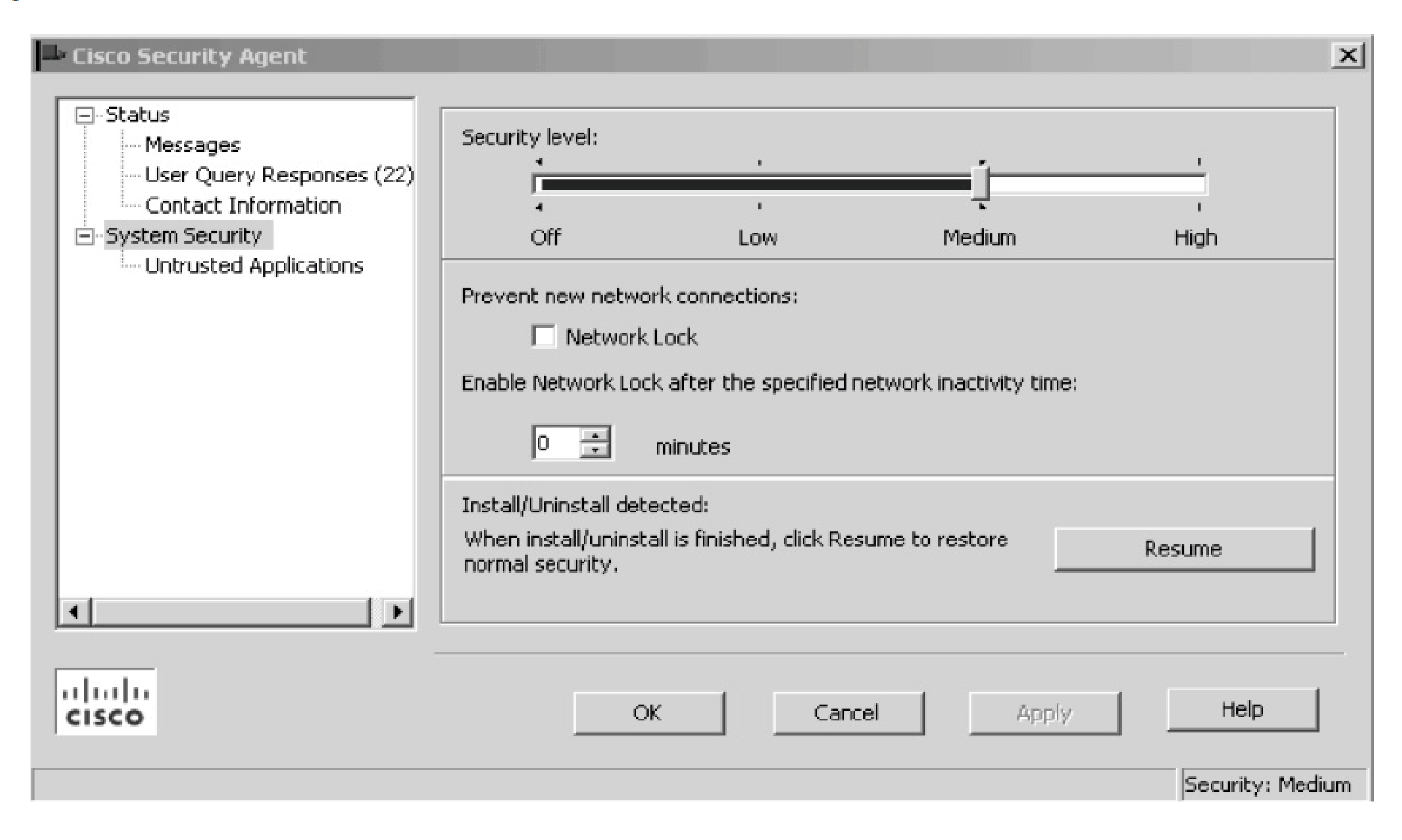


图 7-91　配置 Cisco CSA 客户端

7.4.6 监控 Cisco CSA MC

Cisco CSA MC 提供了大量的日志服务用于监控网络的安全状况，同时还有自带的 CSA 分析器为某个应用环境开发严格的安全策略工具。分析器主要是让 Cisco CSA 软件通过分析终端，确定正在使用的应用和行为的状态。分析器还可以用于在分析终端之后自动生成策略。分析器主要具有两个作用，一是防止应用受到系统影响，二是防止系统受到应用影响。

分析器是一个功能强大的工具，可以根据当前的应用和行为了解终端环境。利用这些信息，可以创建满足某个应用环境的严格要求的策略。定制策略的部署流程包括在默认策略部署中执行的所有任务，以及下面列出的额外任务。在符合下列所有条件时，可以利用 Cisco CSA 分析器创建定制策略。

- ✧ 应用环境的安全要求非常严格。
- ✧ 主机专门用于应用环境(它们不与其他任何应用共享)。
- ✧ 已有针对实际应用服务器的严格变更控制步骤，所有变更都需要得到批准、测试、部署，以及与信息安全和 IT 管理人员的密切协调。
- ✧ 愿意将足够的应用专家和测试资源用于支持思科 CSA 的部署，这些应用专家和测试资源必须是整个分析和策略调节流程的重要组成部分。
- ✧ 愿意为策略定制投入足够的预算(定制策略的开发需要足够的咨询资源和至少三个月的时间)。

使用 Cisco CSA 分析器的第一步是为应用环境的所有重要组件(例如 Web 服务器、Web 应用服务器、应用源代码、数据库、调度系统、操作系统等)找出相关的专家和质量保障资源，必须由相关专家(SME)在策略分析、开发和调节任务中提供协助。

在分析完成之后，可以选择自动创建一个定制策略。所创建的策略可以被导入到 Cisco CSAMC 中。一旦被导入，该分析器策略将会被添加到策略列表中，并将“Job”一词附加到原始分析任务名称中。相关专家随后应当分析该定制策略，并对规则进行调整，他们必须具备对应用环境的广泛了解，以确保定制的规则具有“足够的通用性”，以支持应用此前的执行和在不同情况下的后续执行。在分析器完成了应用分析任务之后，这些规则将会被生成和分发到指定的主机。根据所选择的参数，这些指定主机将在连接到思科 CSAMC 和收到新规则之后，开始执行分析任务。

下面的操作过程，是利用 Cisco CSA MC 获取大量网络设备和服务器的日志来监控网络的安全状况，并实现与 CS-MARS(Mornitoring Analysis Response System，监控分析响应系统)和 IPS(入侵防御系统)联动。对于 CS-MARS 和 IPS 的安装与配置方法请参见后序章节的介绍。

❶ 依次单击 Analysis →Application Behavior Invertigation →Behavior Analyses [Windows]命令，进入行为分析器，如图 7-92 所示。

❷ 创建一个新的分析进程。对于需要分析的行为可以单击 New 按钮添加，并且选择一个主机进行分析，同时还可以定义分析时间，如图 7-93 所示。

❸ 单击 New 按钮后，可以定义一个应用的行为分析，如图 7-94 所示。定义完成后，单击

Save 按钮保存。

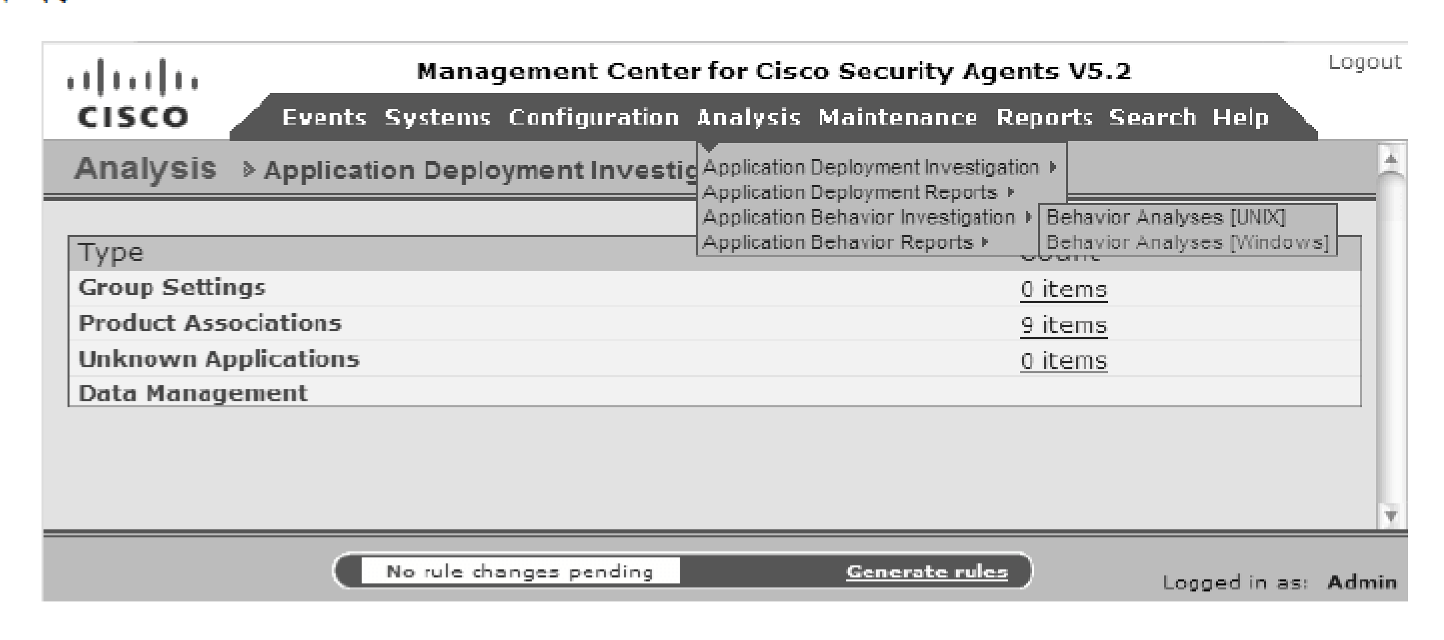


图 7-92　进入行为分析器

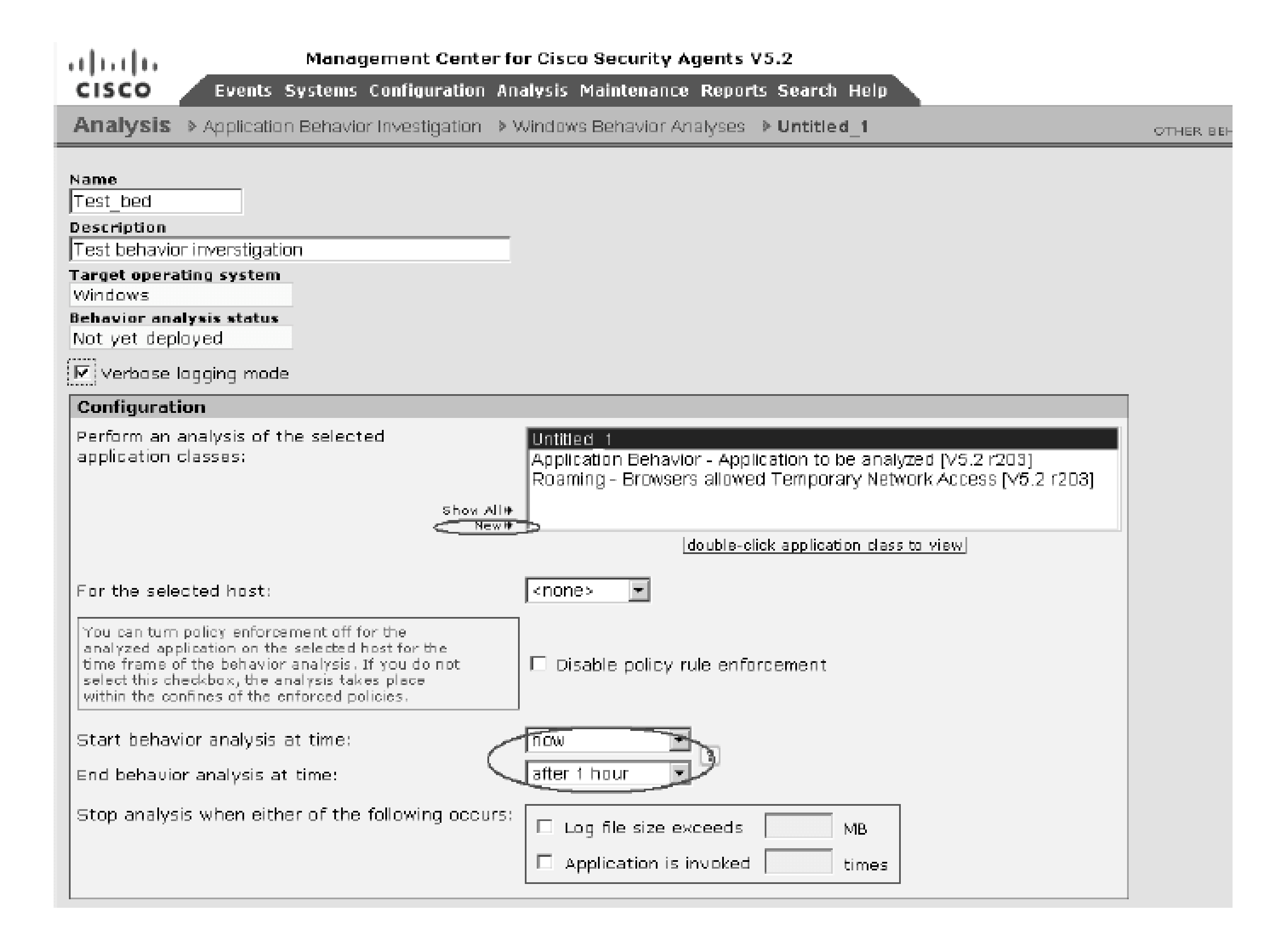


图 7-93　创建新的分析进程

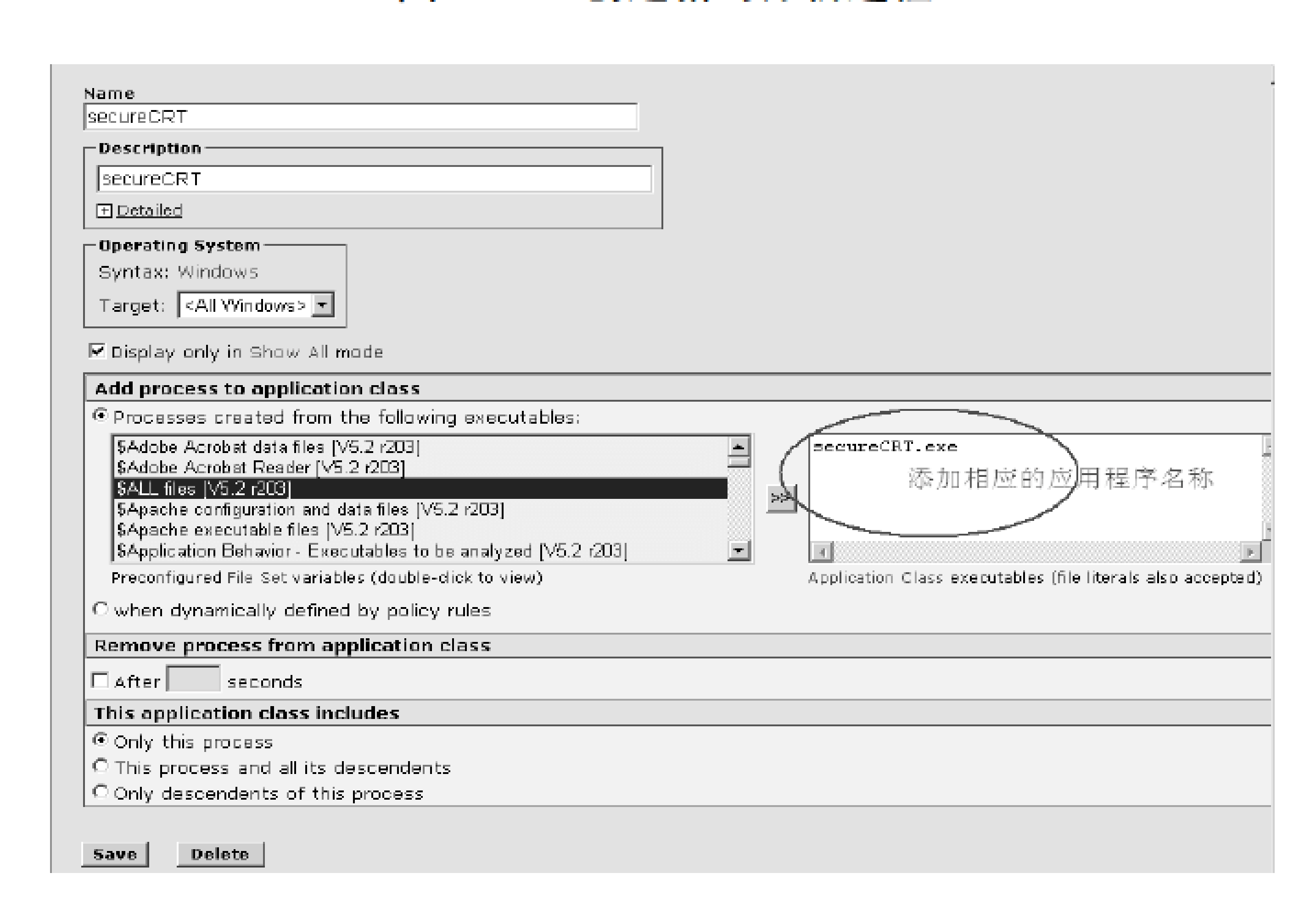


图 7-94　定义新的行为分析

❹ 单击 Generate Rules 按钮，可以部署新的规则。

❺ CSA MC 还可以将报警日志发送到 CS-MARS (Mornitoring Analysis Response System，监控分析响应系统)，用于全局的安全监控和响应。在 MARS 较新的版本中可以自动发现 CSA MC 发送过来的 AGENTS 告警主机，并且把这些 CSA MC 管理的主机放置在网络拓扑图上面。在 CS-MARS 上将 CSA MC 配置为一个事件汇报设备，并且在 CSA MC 上依次单击 Events→Alerts 命令并单击 New 按钮即可创建一个到 MARS 的 SNMP TRAP，如图 7-95 所示。

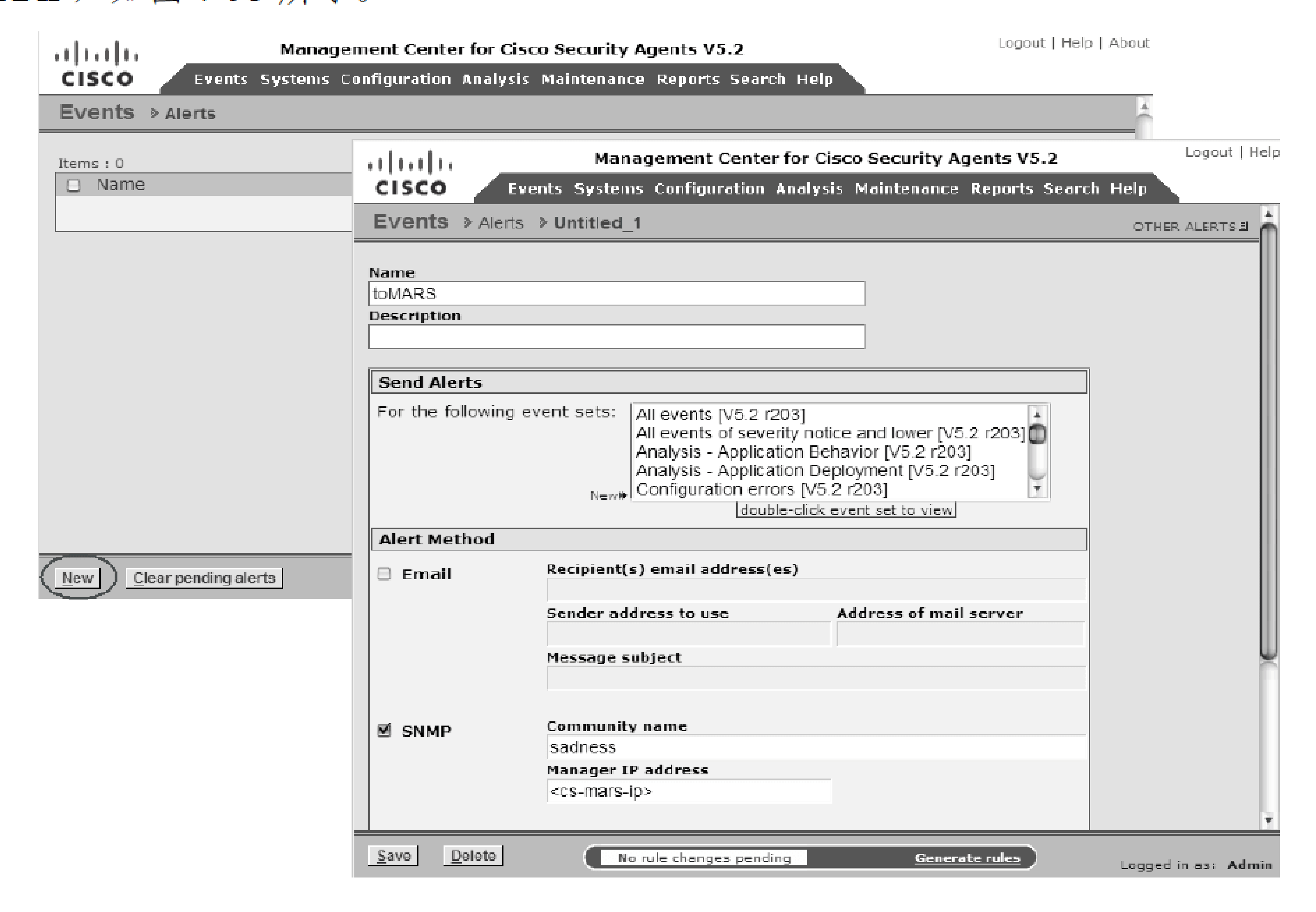


图 7-95　发送日志到 CS-MARS

❻ CSA MC 还可以与 Cisco 入侵防御系统 IPS 配合进行访问控制，CSA MC 可以发送两种类型的信息给 IPS: 主机的 Posture 事件和主机 IP 地址监控列表。IPS 可以根据 CSA MC 发送过来的主机重要信息，进行联动提高防御的准确性。例如，在图 7-96 中，当攻击者扫描一台 CSA 主机端口时，IPS 默认行为是报警，但是当 CSA 将扫描端口信息发送至 CSA MC 后，CSA MC 通过发送消息给 IPS，使 IPS 确认为攻击行为并将攻击阻止。

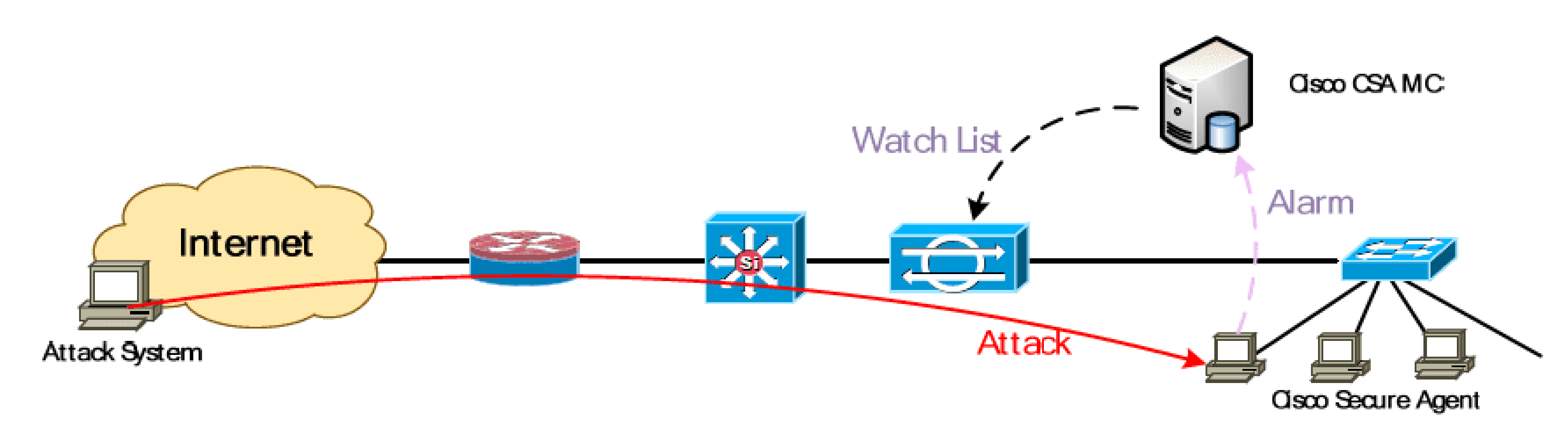


图 7-96　CSA MC 与 IPS 联动

❼ 在 IPS 中，添加 CSA MC 为外部产品接口(External Product Interface)，如图 7-97 所示。

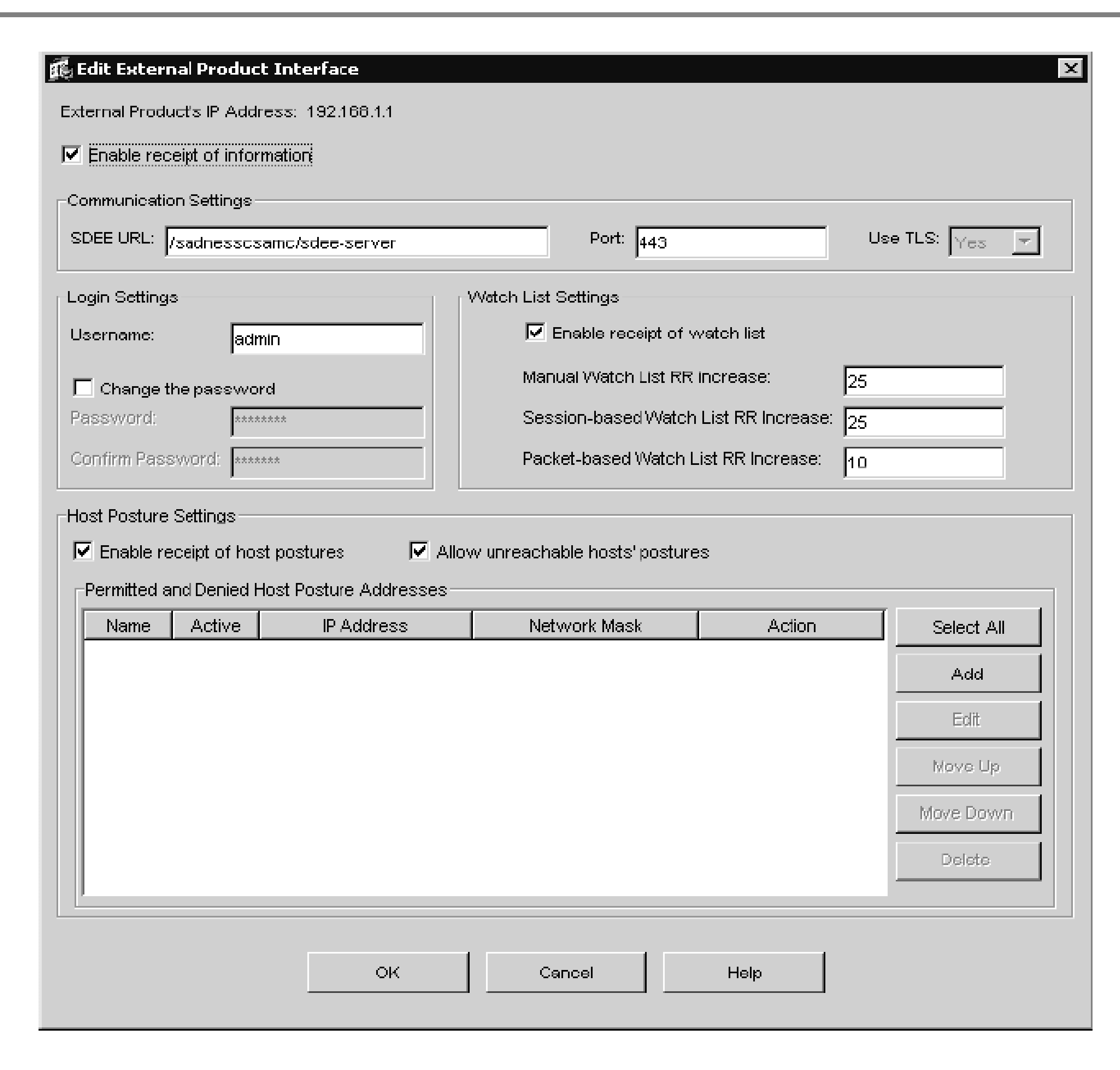


图 7-97　添加 CSA MC 为外部产品接口

❽ 在 IPS 中，添加 CSA MC 为信任主机(Trusted Host)，如图 7-98 所示。

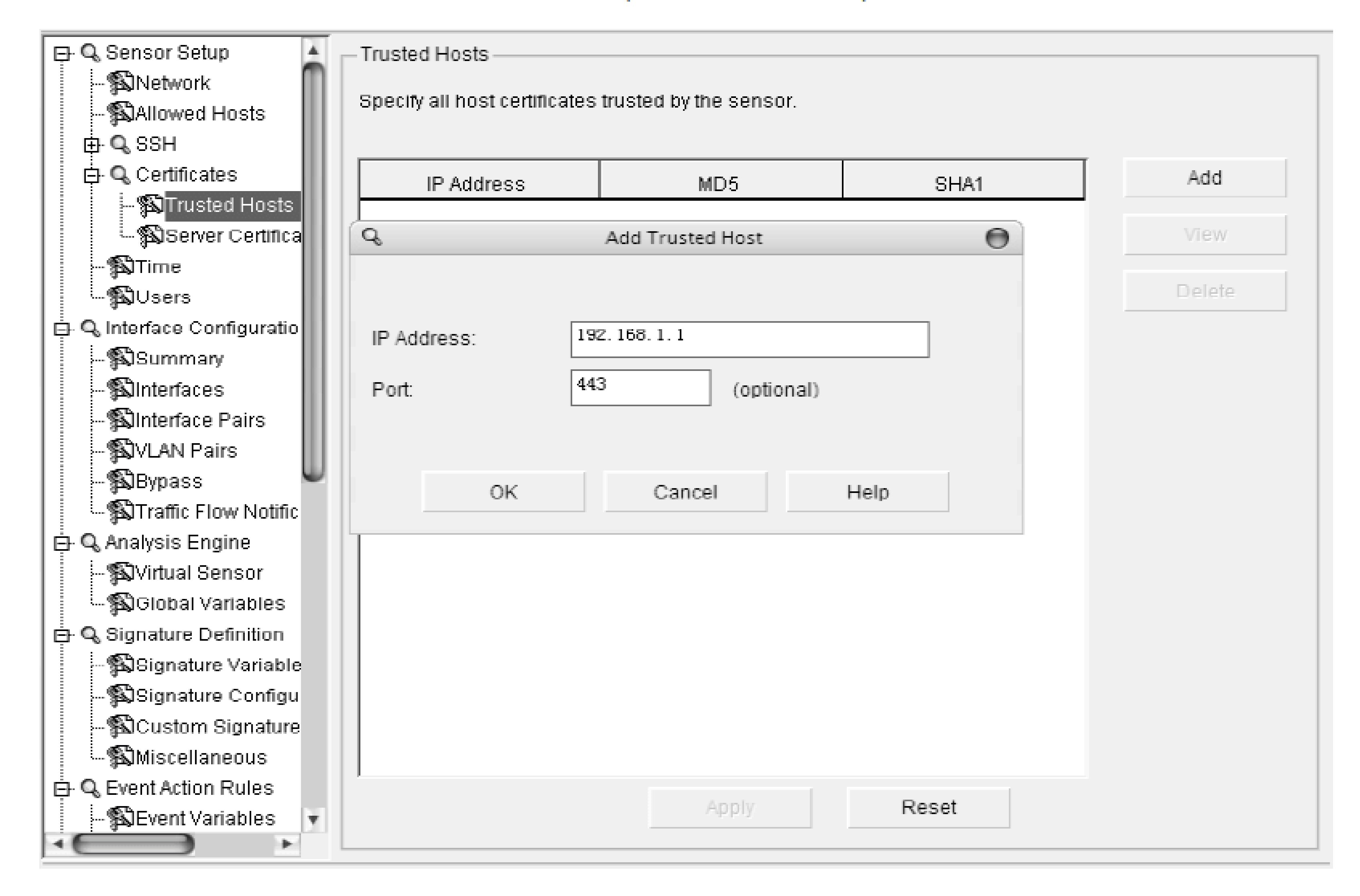


图 7-98　添加 CSA MC 为信任主机

点评与拓展：通过如上的配置，我们完成了基于用户行为检测的防御方案(CSA)。通过对 CSA 和 CSA MC 的配置，并且与 Cisco 安全监控和响应系统(CS-MARS)以及 Cisco IPS 入侵防御系统结合，为服务器创造了一个相对安全的主机环境，通过 CSA MC 集中管理也减轻了管理员的负担。

7.5 本章小结

本章介绍了基于 802.1x 的网络接入控制，并实现了基于 Active Directory 的单一身份登录；然后介绍了 WSUS 自动升级服务器的配置方式，同时通过 Cisco NAC 将两者和防病毒软件等结合起来，为网络提供了一个相对安全的准入规范，减少了带毒主机对网络的影响。本章最后还简要地介绍了基于行为的 CSA，并且可以通过对行为的统计和汇总，有效地防止异常程序的入侵。

下一章我们将介绍传统的网络安全设备——防火墙。

第 8 章　防　火　墙

“防火墙”是一种形象的说法，它是由计算机硬件和软件相组合，在外部网与内部网之间建立起的一个安全网关(Security Gateway)，用于保护内部网免受非法用户的侵入。简单地说，它其实就是一个把互联网与内部网(通常是局域网或城域网)隔开的屏障。

防火墙如果从实现方式上划分，可分为硬件防火墙和软件防火墙两类。通常意义上的防火墙是指硬件防火墙，它通过硬件和软件的结合来达到隔离内、外部网络的目的，价格较贵，但效果较好，一般小型企业和个人很难实现；软件防火墙是通过纯软件的方式来达到防护的目的，价格便宜，但这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。现在的软件防火墙主要有天网的个人版及企业版防火墙、Norton 的个人及企业版防火墙。

通过本章的学习，读者应掌握以下主要内容：

- ✧ 防火墙的分类及工作原理
- ✧ Cisco PIX/ASA 防火墙
- ✧ 微软 ISA 防火墙
- ✧ Linux 防火墙

8.1　防火墙概述

8.1.1　防火墙的硬件平台

通常，按照防火墙硬件平台可以将防火墙分为 x86 架构防火墙、ASIC 架构防火墙和 NP 架构防火墙三类。

1. x86 架构防火墙

x86 架构防火墙采用通用 CPU 和 PCI 总线接口，具有很高的灵活性和可扩展性，过去一直是防火墙开发的主要平台。其产品功能主要由软件实现，可以根据用户的实际需要而相应地调整，增加或减少功能模块，产品比较灵活，功能十分丰富。最初的千兆防火墙是基于 x86 架构。

作为通用的计算平台，x86 架构的结构层次较多，不易优化，且往往会受到 PCI 总线的带宽限制。虽然 PCI 总线接口理论上能达到接近 2 Gbps 的吞吐量，但是通用 CPU 的处理能力有限，尽管防火墙软件部分可以尽可能地优化，很难达到千兆速率。同时很多 x86 架构的防火墙是基于定制的通用操作系统，安全性很大程度上取决于通用操作系统自身的安全性，可能会存在安全漏洞。

基于 x86 架构防火墙的典型代表是 Cisco 系统防火墙，图 8-1 所示为 Cisco ASA 系列防火墙产品。



图 8-1　Cisco ASA 防火墙

2. ASIC 架构防火墙

相比之下，ASIC 架构防火墙通过专门设计的 ASIC 芯片进行硬件加速处理。ASIC 通过把指令或计算逻辑固化到芯片中，获得了很高的处理能力，因而明显提升了防火墙的性能。新一代的高可编程 ASIC 采用了更灵活的设计，能够通过软件改变应用逻辑，具有更广泛的适应能力。但是，ASIC 的缺点也同样明显，其灵活性和扩展性不够，开发费用高，开发周期太长。

虽然研发成本较高，灵活性受限制，无法支持太多的功能，但其具有先天的优势，非常适合应用于模式简单、对吞吐量和时延指标要求较高的电信级大流量的处理。

ASIC 架构防火墙以 Juniper 公司的 NetScreen 产品为代表，如图 8-2 所示。



图 8-2　NetScreen 防火墙

3. NP 架构防火墙

NP 架构可以说是介于 x86 架构与 ASIC 架构之间的技术，NP 是专门为网络设备处理网络流量而设计的处理器，其体系结构和指令集对于防火墙常用的包过滤、转发等算法和操作都进行了专门的优化，可以高效地完成 TCP/IP 栈的常用操作，并对网络流量进行快速的并发处理。硬件结构设计也大多采用高速的接口技术和总线规范，具有较高的 I/O 能力。它可以构建一种硬件加速的完全可编程的架构，这种架构的软硬件都易于升级，软件可以支持新的标准和协议，硬件设计支持更高的网络速度，从而使产品的生命周期更长。由于防火墙处理的就是网络数据包，所以基于 NP 架构的防火墙与 x86 架构的防火墙相比，性能得到了很大的提高。

NP 架构通过专门的指令集和配套的软件开发系统，提供强大的编程能力，因而便于开发应用，支持可扩展的服务，而且研制周期短、成本较低。但是，与 x86 架构相比，由于

应用开发、功能扩展受到 NP 架构的配套软件的限制，基于 NP 技术的防火墙的灵活性要差一些。由于依赖软件环境，所以在性能方面 NP 不如 ASIC。NP 架构开发的难度和灵活性都介于 ASIC 架构和 x86 构架之间，应该说，NP 是 x86 架构和 ASIC 架构一个折中。

NP 架构主要出现在国内很多厂商的防火墙设备上，例如东软 NetEye 防火墙，如图 8-3 所示。



图 8-3　东软 NP 防火墙

从上面的分析可以看出，x86 架构、NP 架构和 ASIC 架构各有优缺点。x86 架构灵活性最高，新功能、新模块扩展容易，但性能肯定满足不了千兆需要。ASIC 架构性能最高，千兆、万兆吞吐速率均可实现，但灵活性最低，定型后再扩展十分困难。NP 架构则介于两者之间，性能可满足千兆需要，同时也具有一定的灵活性。

8.1.2　防火墙的体系结构

根据处理数据的方式，防火墙通常可分为主机防火墙、包过滤防火墙、电路层防火墙、应用代理防火墙、状态检测防火墙等几类。

1. 主机防火墙

主机防火墙通常是为保护单一主机而建立的防火墙，可以看做主机的外壳。通常这种防火墙通过使用者定义的允许出站、入站的流量规则进行过滤，并且很多公司的产品默认支持不同等级的防范策略。即便是在 Linux 中，安装时同样可以选择基于 Iptables 的防火墙产品。但是对于一个大型网络而言，虽然每台主机都拥有防火墙，但却无法及时地对这些防火墙的策略进行同步，因此安全漏洞极大。

2. 包过滤防火墙

通常包过滤防火墙基于一些网络设备(如路由器、交换机等)，通过一系列访问控制列表(Access List，ACL)来控制数据包的转发策略。通常这些策略工作在 OSI 模型的网络层，如图 8-4 所示。

包过滤防火墙的优点是：不用改动应用程序；一个过滤路由器能协助保护整个网络；数据包过滤对用户透明；过滤路由器速度快、效率高。但缺点也很明显，它不能彻底防止地址欺骗；一些应用协议不适合于数据包过滤；正常的数据包过滤路由器无法执行某些安全策略；安全性较差；数据包工具存在很多局限性。

在某些情况下包过滤防火墙可以用于攻击的应急处理，以及某些应用的过滤。在后面的例子中将会详细介绍。

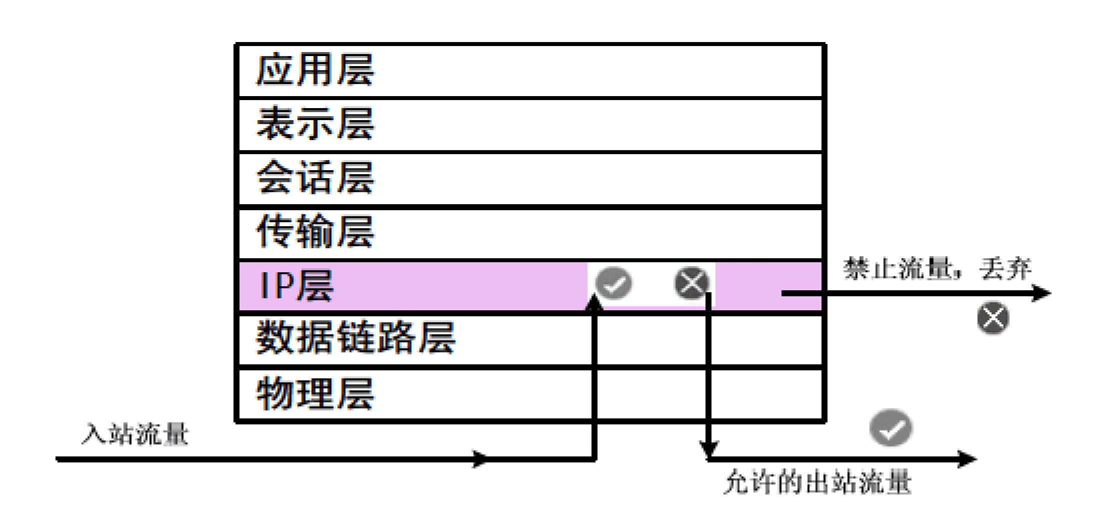


图 8-4　包过滤防火墙

3. 电路层防火墙

电路层防火墙通常工作在 OSI 模型的第五层(会话层图 8-5)，它通过监控会话建立得是否合理来进行相应的过滤。这种模式，仅在内部链接和外部链接之间来回复制字节，因此所有的会话均起源于这个防火墙；对于外部网络而言，起到了隐藏内部网络细节的作用。

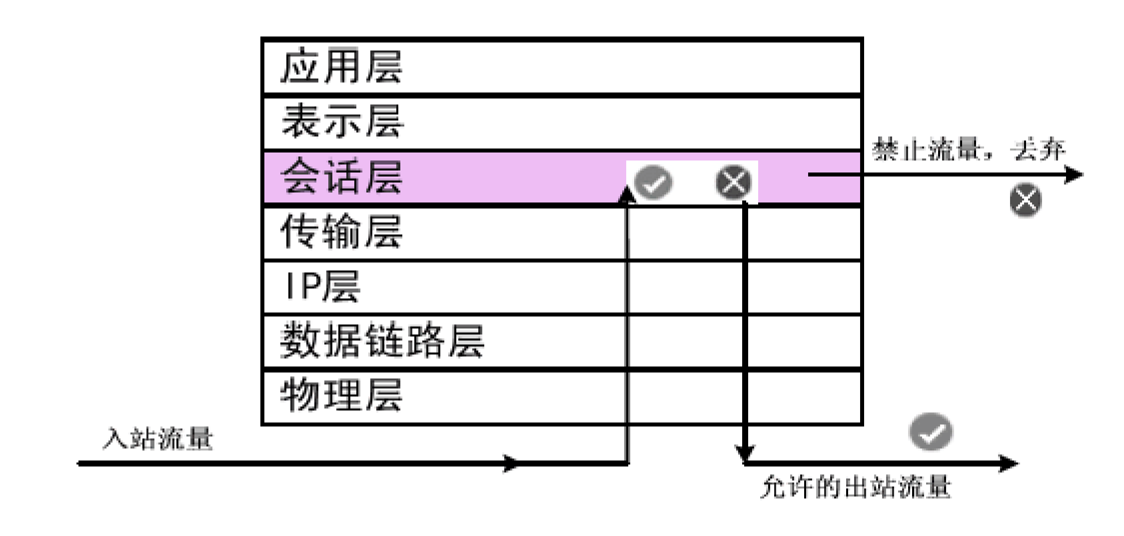


图 8-5　电路层防火墙

4. 应用代理防火墙

通常应用代理防火墙工作在 OSI 模型的应用层(图 8-6)，和我们常说的代理服务器原理相同，并且防火墙需要为每一种服务器创建一个进程，让外部网络看上去是在运行一个终端系统，并通过一系列进程映射，将对外会话和对内会话联系起来。它还可用来保持一个所有应用程序使用的记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一。

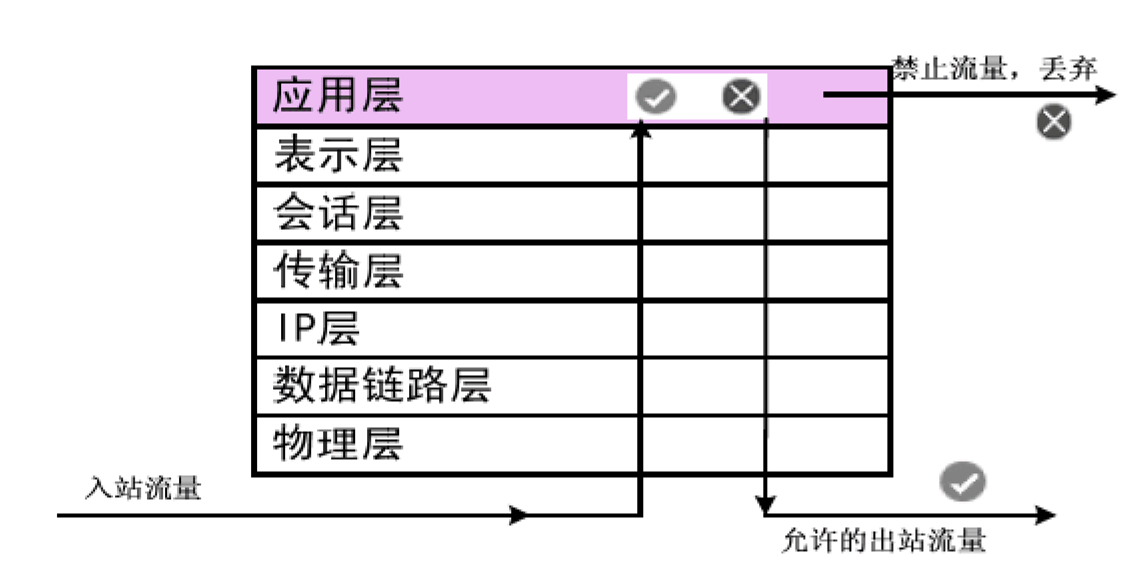


图 8-6　应用代理防火墙

5. 状态检测防火墙

状态检测防火墙(图 8-7)通过对 OSI 模型顶部 4 层的策略分析进行过滤，相当于以上三种防火墙的结合体。状态检测防火墙虽然集成了前三者的特点，但它实现应用层防火墙的模式与前面三种不同。状态检测防火墙并不破坏客户机/服务器模型来分析应用层数据，它允许受信任的客户机和不受信任的主机进行直接通信。从理论上讲，状态检测防火墙拥有更高的安全性。

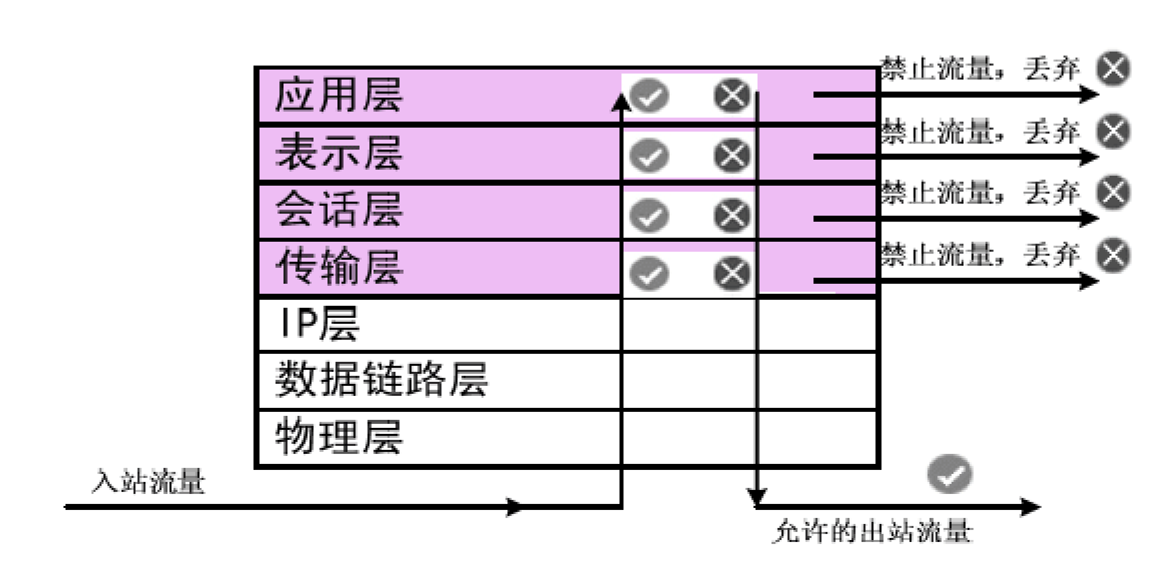


图 8-7　状态检测防火墙

8.1.3　防火墙的部署方式

通常防火墙的部署方式有两种，一种是区域分割的三角方式，另一种是防火墙层叠方式。

1. 区域分割的三角方式

区域分割的三角方式是指将网络分为内部网络(军事化区域)、外部网络和 DMZ 区域。例如，将 Web 服务器、邮件服务器、DNS 服务器、前台查询计算机等放置在 DMZ 区域，而内部的文件服务器、数据库服务器等关键应用都放置在内部网络中，从而使它们受到良好的保护，图 8-8 所示为以区域分割的三角方式创建 DMZ。

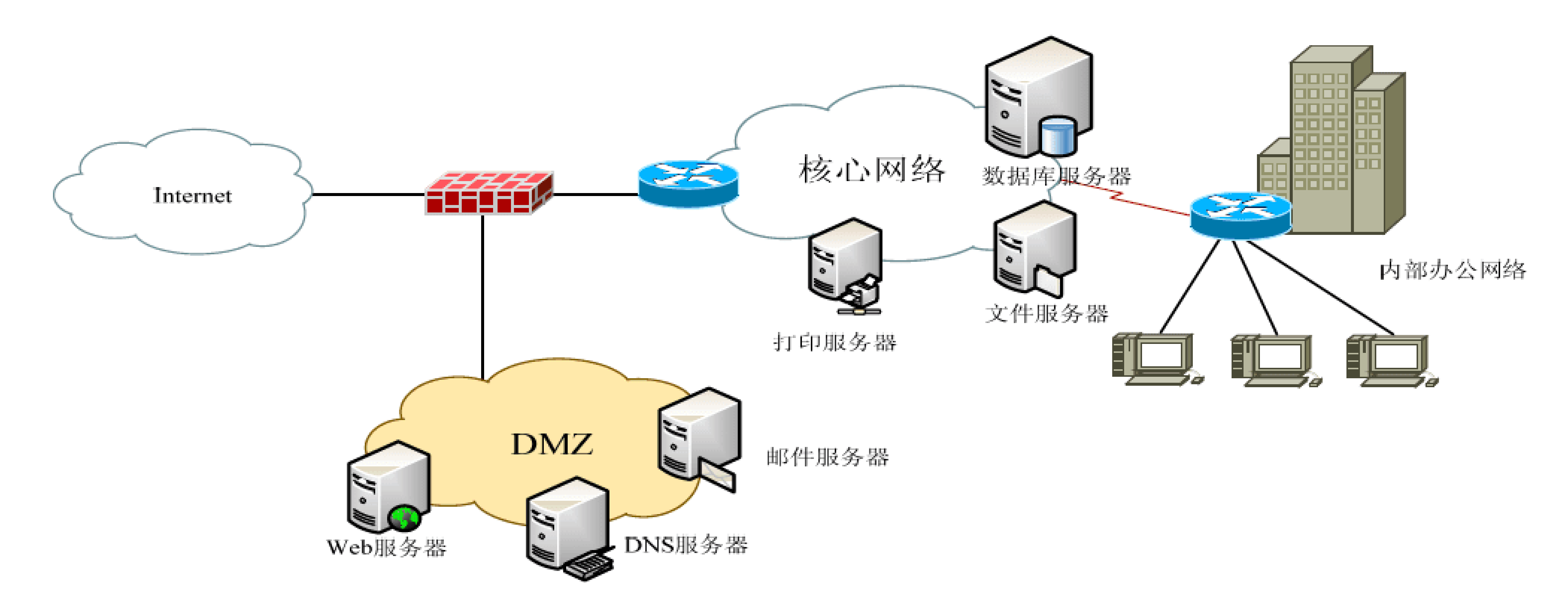


图 8-8　以区域分割的三角方式创建 DMZ

2. 防火墙层叠方式

与区域分割的三角方式不同，防火墙层叠方式使用两台防火墙，并将 DMZ 区域放置在两台防火墙之间，如图 8-9 所示。其中，连接外部网络和 DMZ 区域的防火墙仅仅做一些包过滤，通常由边界路由器的访问控制列表来实现，而连接内部网络和 DMZ 区域的防火墙是一台专用防火墙，实施详细的访问控制策略。

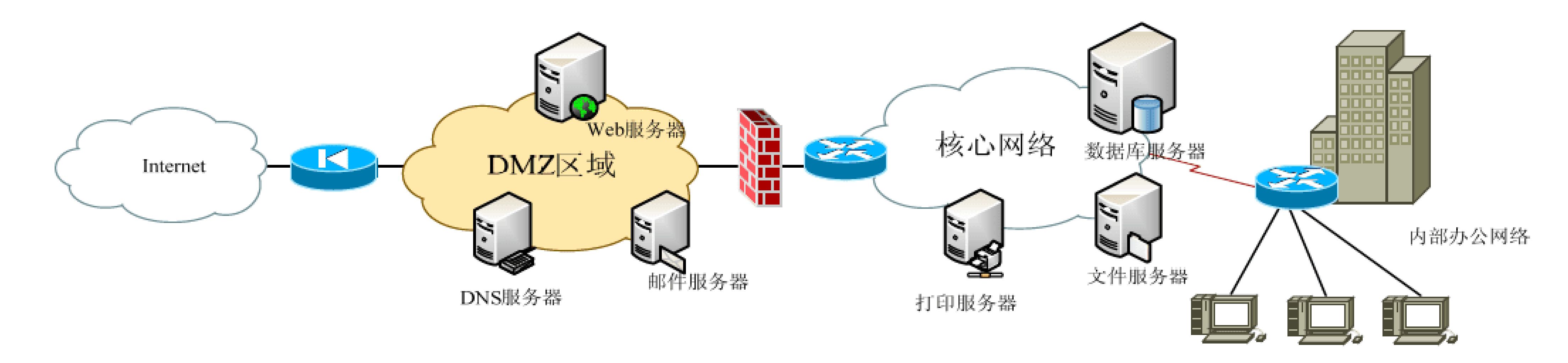


图 8-9　防火墙层叠方式

8.2　Cisco IOS 防火墙

应用实例导航：利用 ACL 为 Sadness 公司部署简单的防火墙

※场景呈现

Sadness 公司遭受到来自外界的大量碎片(Fragments)攻击，同时还伴随着大量的 ICMP 报文和 TCP SYN 攻击。同时，为了限制员工使用 Internet，公司主管希望限制员工仅能在午饭休息时间或者前后几个小时内使用外部网络，其他时间只能使用内部网络。图 8-10 所示为 Sadness 公司的网络边界拓扑。

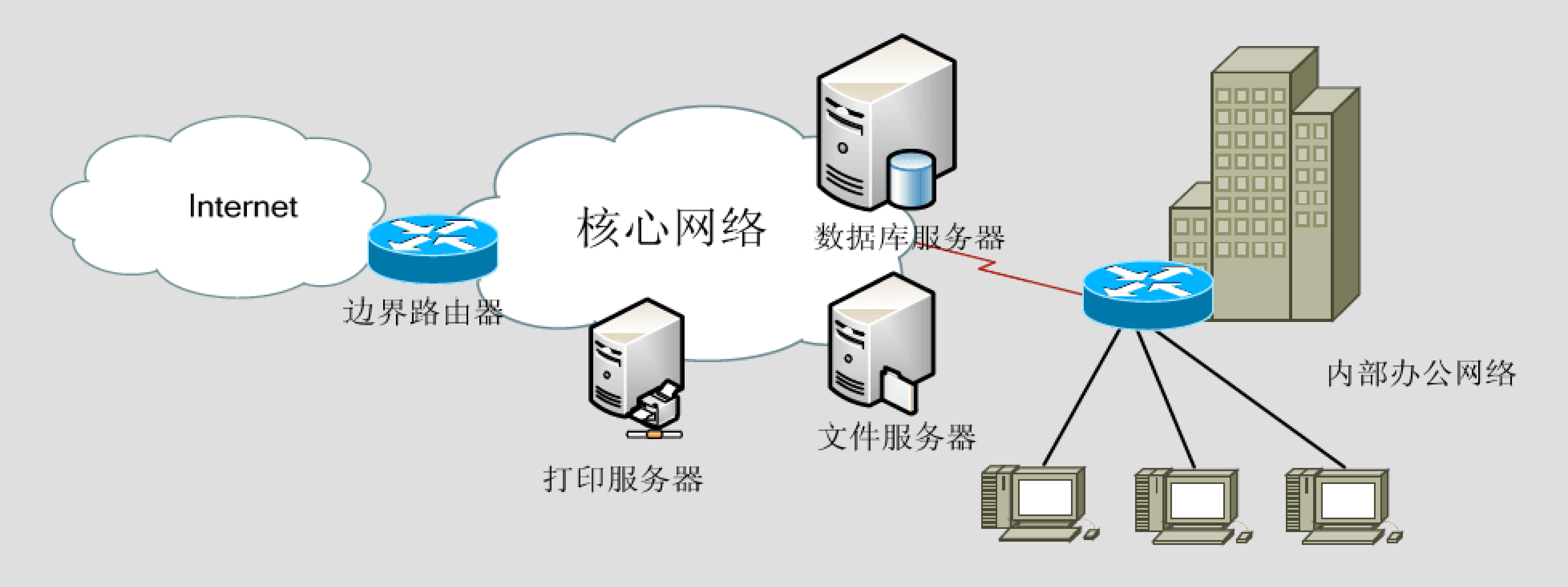


图 8-10　Sadness 公司的网络边界拓扑

虽然提出了许多要求，但公司却没有足够的经费进行网络升级和改造，因此公司领导希望网络管理员 Jam 能够通过廉价的方式满足这些要求。Jam 通过使用边界的 Cisco 路由器



内置的一些防火墙功能了满足公司的需求。

※技术要领

(1) 基于访问控制列表过滤的配置方法；
(2) 基于上下文的访问控制的配置方法；
(3) 基于网络应用识别的配置方法。

随着网络的逐渐发展，Cisco 在运行 IOS 软件的路由器上也支持更多的安全特性，Cisco IOS 防火墙特性集为每一个网络周边集成了稳健的防火墙功能和入侵检测，丰富了 Cisco IOS 的安全功能。如果与 Cisco IOS IPSec 软件和其他基于 Cisco IOS 软件的技术(例如 L2TP 隧道和服务质量(QoS))相结合，Cisco IOS 防火墙特性集可以提供一个全面、集成的虚拟专用网络(VPN)解决方案。Cisco IOS 软件可用在广泛的 Cisco 路由器平台上，允许客户根据带宽、LAN/WAN 密度和多种服务需求选择路由器平台，同时从先进的安全性受益。Cisco IOS 防火墙具有如下特征。

- 基于上下文的访问控制(CBAC)能提供基于应用程序的安全筛选，并支持最新协议。
- Java 过滤功能防止下载动机不纯的小应用程序。
- 可以在现有功能基础上添加拒绝服务探测和预防功能，从而增强网络的保护能力。
- 可以在探测到可疑行为后，向中央管理控制台实时发送警报和系统记录错误信息。
- TCP/UDP 事务处理记录可以按源/目的地址和端口对来跟踪用户访问。

8.2.1 基于访问控制列表过滤

访问控制列表(Access Control List，ACL) 是路由器接口的指令列表，用来控制端口进出的数据包。访问控制列表就是一系列允许和拒绝条件的集合，通过访问控制列表可以过滤发进和发出的信息包的请求，实现对路由器和网络的安全控制。路由器一个一个地检测包与访问控制列表的条件，在满足第一个匹配条件后，就可以决定路由器接收或拒收该包。

ACL 适用于所有的包路由协议，如 IP、IPX、AppleTalk 等。ACL 的定义也是基于每一种协议的。如果路由器接口配置成为支持三种协议(IP、AppleTalk 以及 IPX)，那么，用户必须定义三种 ACL 来分别控制遵循这三种协议的数据包。

ACL 可以限制网络流量，提高网络性能，例如可以根据数据包的协议指定数据包的优先级；提供对通信流量的控制手段，例如 ACL 可以限定或简化路由更新信息的长度，从而限制通过路由器某一网段的通信流量；提供网络安全访问的基本手段，例如只允许主主机 A 访问人力资源网络，而拒绝主机 B 访问；可以在路由器端口处决定哪种类型的通信流量被转发或被阻塞，例如用户可以允许 E-mail 通信流量被路由，而拒绝所有的 Telnet 通信流量。

目前有两种主要的 ACL：标准 ACL 和扩展 ACL。两者主要的区别是，标准 ACL 只检查数据包的源地址；扩展 ACL 既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。

由于目前网络主要是使用 TCP/IP，本书只介绍标准 IP 访问控制列表(编号范围是 1～99)和扩展 IP 访问控制列表(编号范围是 100～199)，而对 IPX/SPX 数据包进行过滤的标准 IPX

访问控制列表(编号范围是 800～899)和扩展 IPX 访问控制列表(编号范围是 900～999)不作介绍。

除了用编号来代表一个 ACL 外，在 Cisco IOS11.2 以后的版本中，还可以以列表名代替列表编号来定义访问控制列表，这种访问控制列表称为命名访问控制列表。命名访问控制列表同样包括标准和扩展两种列表，定义过滤的语句与编号方式中相似。

ACL 通过过滤数据包并且丢弃不希望抵达目的地的数据包来控制通信流量。然而，网络能否有效地减少不必要的通信流量，还要取决于网络管理员把 ACL 放置在哪个地方。一般来说，标准 ACL 要尽量靠近目的端，而扩展 ACL 要尽量靠近源端。

ACL 的配置分为两个步骤。

第一步是在全局配置模式下，使用 access-list 命令创建 ACL。

```
Router (config)# access-list access-list-number {permit | deny } {test-conditions}
    //其中，access-list-number为ACL的表号。
```

第二步是在接口配置模式下，使用 access-group 命令定义 ACL 应用到某一接口上。

```
Router (config-if)# {protocol} access-group access-list-number {in | out }
//其中，in和out参数可以控制接口中不同方向的数据包。如果不配置该参数，默认为out
```

ACL 在一个接口可以进行双向控制，即配置两条命令，一条为 in，另一条为 out，两条命令执行的 ACL 表号可以相同，也可以不同。但是，在一个接口的一个方向上，只能有一个 ACL 控制。

点评与拓展： 在进行 ACL 配置时，一定要先在全局配置模式下配置 ACL 表，然后在具体接口上进行配置；否则会造成网络的安全隐患。

1. 利用 ACL 过滤特定的报文

针对应用实例导航中所述的报文碎片攻击、ICMP 攻击和 TCP SYN 攻击，可以通过配置 ACL 来过滤这些报文，以减少这些攻击。

❶ 为了防范报文碎片攻击，可以过滤所有不完整的 IP 报文。方法如下。

```
Router(config)# access-list 139 deny ip any any fragments
```

❷ 为了防范 ICMP 攻击，可以过滤所有的 ICMP 报文。方法如下。

```
Router(config)#access-list 139 deny icmp any any  //过滤所有ICMP报文
```

若仅需要过滤 ping 包，而允许其他 ICMP 报文，可以按下述方法配置。

```
Router(config)#access-list 139 deny icmp any any echo
Router(config)#access-list 139 deny icmp any any echo-reply
```

❸ 为了防范 TCP SYN 攻击，可以过滤所有的半连接。方法如下(注：为了展示命名 ACL 的定义方法，这里定义了一个命名 ACL)。

```
Router(config)# ip access-list extended tcp-syn-flood
Router(config-ext-nacl)# permit tcp any 10.0.1.0 0.0.255.255 established
```

❹ 完成 ACL 定义后，需要将 ACL 应用到相应的接口。

```
Router(config)# interface ethernet1
Router(config-if)# ip access-group tcp-syn-flood in    //应用命名ACL
Router(config-if)# ip access-group 139 out        //应用编号ACL
```

2. 利用 ACL 应对网络攻击

Sadness 公司在某日发现其广域网带宽全部耗尽，各种服务运行缓慢。后来接到 ISP 的责难电话，询问为什么要攻击 ISP 接入路由器。Sadness 公司对此进行了查找，发现大量未知 IP 地址通过 Sadness 公司网络对外发送大量报文。事后发现是黑客攻破了一台 Sadness 内部网络的主机，并在该主机使用伪造的源 IP 地址对运营商的路由器进行攻击。Jam 在边界路由器上做了如下配置。

❶ 将各种攻击常用的地址段进行了屏蔽，只让合法的 IP 地址对外发送流量。

```
Router(config)# ip access-list extended egress-acl
Router(config-ext-nacl)# deny ip any 1.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 2.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 5.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 7.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 23.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 27.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 172.16.0.0 0.15.255.255
Router(config-ext-nacl)# deny ip any 192.168.0.0 0.0.255.255
Router(config-ext-nacl)# deny ip any 224.0.0.0 15.255.255.255
Router(config-ext-nacl)# deny ip any 240.0.0.0 15.255.255.255
Router(config-ext-nacl)# deny ip any 0.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 169.254.0.0 0.0.255.255
Router(config-ext-nacl)# deny ip any 192.0.2.0 0.0.0.255
Router(config-ext-nacl)# permit ip 46.1.0.0 0.0.255.255 any
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group egress-acl out
```

❷ 为了防止内部人员对外部网络进行攻击，还需要限制发出的 ICMP 流量和 traceroute 流量。

```
Router(config)# ip access-list extended ICMP-traceroute
Router(config-ext-nacl)# permit icmp host 46.1.2.3 any echo
Router(config-ext-nacl)#   permit   icmp   46.1.0.0   0.0.255.255   any
parameter-problem
Router(config-ext-nacl)#permit icmp 46.1.0.0 0.0.255.255 any packet-too-big
Router(config-ext-nacl)# permit icmp 46.1.0.0 0.0.255.255 any source-quench
Router(config-ext-nacl)# deny icmp any any
Router(config-ext-nacl)# deny udp any any range 33400 34400
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group ICMP-traceroute out
```

3. 利用 ACL 阻止不必要的服务

通常公司内部容易造成安全威胁的软件是各类即时通信产品(如 QQ、MSN)，同时大量的 P2P 应用(如 BT、电驴等)会导致带宽拥塞，因此需要阻止这些不必要的网络服务。

禁止使用 MSN、电驴的配置过程如下。

❶ 如果 Sadness 公司不希望员工使用 MSN，可以通过 ACL 来禁用这个服务。

```
Router(config)# ip access-list extended MSN
```

```
Router(config-ext-nacl)# deny tcp any any eq 1503
Router(config-ext-nacl)# deny tcp any any eq 1863
Router(config-ext-nacl)# deny tcp any any eq 6891
Router(config-ext-nacl)# deny udp any any eq 1863
Router(config-ext-nacl)# deny udp any any range 13324 13325
Router(config-ext-nacl)# deny tcp any any eq 569
Router(config-ext-nacl)# deny udp any any eq 569
Router(config-ext-nacl)# deny ip any 64.4.13.0 0.0.0.255
Router(config-ext-nacl)# deny ip any host 207.46.104.20
Router(config-ext-nacl)# deny ip any 207.46.96.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group MSN out
```

❷ 如果 Sadness 公司不希望员工使用电驴，也可以通过 ACL 进行过滤。对于其他 P2P 协议(如 BT 等)，在下一节介绍 NBAR 的时候再进行配置。

```
Router(config)# ip access-list extended banedonkey
Router(config-ext-nacl)# deny tcp any any range 4661 4662
Router(config-ext-nacl)# deny tcp any any range 4242 4243
Router(config-ext-nacl)# deny udp any any eq 4665
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group banedonkey in
Router(config-if)# ip access-group banedonkey out
```

4. 配置定时 ACL

例如，管理员希望每周工作日的 8 :00—18 :00 不准 WWW 流量通过，周末从中午到 16:00 不准 UDP 流量通过，2008 年国庆节(10 月 1 日—10 月 7 日)期间，不准任何流量通过。其配置方式如下。

```
Router(config)#time-range weekdays
Router(config-time-range)#period weekdays 8:00 to 18:00
Router(config)#time-range weekend
Router(config-time-range)#period weekend 12:00 to 16:00
Router(config)#time-range nationalday
Router(config-time-range)#absolute start 8:00 1 Oct 2008 end 8:00 8 Oct 2008
Router(config)#access-list 110 deny tcp any any eq www time-range weekdays
Router(config)#access-list 110 deny udp any any  time-range weekend
Router(config)#access-list 110 deny ip any any time-range nationalday
Router(config)# interface ethernet1
Router(config-if)# ip access-group 110 in
```

其中，time-range 可以使用 periodic 定义一个周期，也可以使用 absolute 定义一个时间段。

5. 配置动态 ACL

动态 ACL 能够允许用户在通过路由器认证之后进行临时性的访问。例如 Sadness 公司的网络出现故障，需要 Cisco TAC 的工程师远程登录来检查网络故障时，可以使用这种方式。假设 Cisco TAC 工程师所使用的 IP 地址为 64.1.1.1，Sadness 公司的边界路由器的 IP 地址为 46.1.2.3，其配置方式如下。

❶ 定义一个用户名和密码，并加上 autocommand 和 timeout 参数，这些参数必须和动态 ACL 中指定的超时值相匹配。

```
Router(config)# username Cisco password CiscoTAC
Router(config)# username Cisco autocommand access-enable timeout 5
```

❷ 定义一个仅有一行的动态 ACL，指定用户在通过认证后才能传输数据，同时此行设置一个超时值，应与上述匹配。定义一个扩展 ACL，其范围和动态 ACL 一样，用该 ACL 对接口进行常规数据流量过滤，并允许该接口的 Telnet 访问。ACL 定义完成后，将其应用到相应的网络接口上。

```
Router(config)#access-list 101 dynamic allowTAC timeout 5 permit ip 46.1.2.0
0.0.0.255 any
Router(config)#access-list 101 permit tcp 64.1.1.0 0.0.0.255 host 46.1.2.3
eq telnet
```

❸ 将 login local 加到 vty 虚拟接口上，这样 Cisco TAC 的工程师就能够远程登录到公司的路由器上并检查网络故障了。

```
Router(config)#line vty 0 4
Router(config-line)#login local
```

点评与拓展：CISCO 对于配置动态 ACL 有如下规则和建议。

✧ 对于超时，可以通过 autocommand 后加 access-enable 来定义，也可以用 ACL 中的 timeout 来定义。空闲超时和绝对超时(ACL 的那个时间)必须定义，否则，临时性的访问 ACL 将无限期地常驻在接口上。

✧ 如果要配置一个空闲超时，其值应等于拨号空闲超时值，空闲超时应小于绝对超时。

8.2.2　基于上下文的访问控制

基于上下文的访问控制(Context-Based Access Control，CBAC)提供了一种流量过滤功能，同时可用作网络防火墙的智能部分。

1. CBAC 的主要功能

CBAC 能为网络提供流量过滤、流量检查、警报和审计、入侵检测等多种网络保护功能。

1)　流量过滤

CBAC 智能地基于应用层协议会话信息过滤 TCP 和 UDP 包，可以配置 CBAC 来允许指定的 TCP 和 UDP 流量仅当连接由保护的网络中发起时穿过防火墙。CBAC 可以拦截起源于防火墙任意方向的流量，而且 CBAC 可以用在内部网络、外部网络和互联网边缘。

没有 CBAC，流量过滤仅限于在网络层检查访问列表，或者最多在传输层检查访问列表。CBAC 检查的不仅是网络层和传输层的信息，也检查应用层的信息(例如 FTP 连接信息)，检测会话的状态信息，这就允许支持多通道协商的协议。大多数多媒体协议例如 FTP.rpc)就有多通道参与。

使用 CBAC 进行 Java 封锁，可以配置用来基于服务器地址或者完全地拒绝镶嵌了压缩包的 Java 小程序。使用 Java，必须保护用户下载使用它们的时候避免网络造成不良风险。

为了更好地保护网络，降低风险，需要所有用户在其浏览器中禁用 Java。如果这个方案不可行，可以建立一个 CBAC 拦截规则在防火墙过滤，如果是用户必须使用的 Java 程序就放行。如果要进行更广泛的 Java、Active-X 内容过滤或者病毒扫描，则应该考虑购买指定的过滤产品。

2) 流量检查

CBAC 通过检查穿过防火墙的流量来探索和管理 TCP 和 UDP 会话的状态信息。这个状态信息是用来建立临时通道打开防火墙的 ACL 允许的流量返回，以及允许会话的附加数据连接。

在应用层检查包，维护 TCP 和 UDP 会话信息，提供给 CBAC 探测和阻止一定类型网络攻击(如 SYN-Flooding)的能力。SYN-Flooding 攻击产生在网络攻击者用半开的连接持续连接服务器的时候，导致对正常的服务请求拒绝。

CBAC 帮助防止受到 DoS 攻击。CBAC 监视 TCP 连接中的包状态序列号来看是否它们已越位，CBAC 可以扔掉任意的数据包，当然也可以配置 CBAC 扔掉半开连接，那就需要更多的处理器和内存资源。另外，CBAC 可以探测少数非正常速率的新连接，而且还能发出警告信息。

CBAC 也能保护基于碎片的 DoS 攻击。尽管防火墙能阻止攻击者连接到假设主机，攻击者仍然可以瓦解这个主机提供的服务。这是用发送许多非初始的 IP 分段或者发送完整分段包穿过只过滤分段的第一段包的路由器。这些分段可以绑定一些可以从新组装的包的一些信息。

3) 警报和审计

CBAC 也能生成实时警报和审计痕迹，加强审计特性，用 Syslog 来跟踪所有网络处理情况，记录时间戳、源/目的端口号和传输字节的总数，更高级的还有基于会话的报告。实时警报基于积极地探测可疑情况发送 Syslog 错误信息到中央管理控制台。使用 CBAC 监视规则，可以基于每一个协议配置警报和跟踪信息。例如，想要生成关于 HTTP 流量的跟踪信息，可以在 CBAC 规则中加入指定的条目。

4) 入侵检测

CBAC 提供一种有限的入侵检测以保护指定的 SMTP 攻击。使用入侵检测，Syslog 信息显示和监控指定的“攻击特征”。特定的网络攻击类型有指定的角色或特征。当 CBAC 检测到攻击，便复位有关连接，将系统日志发送到 Syslog 服务器。

CBAC 提供附加的有限的入侵检测，Cisco IOS 防火墙特性集提供入侵检测技术给中等级别和高端路由器平台使用 Cisco IOS 防火墙 IDS。这里考虑到网络大小，尤其是路由器作为附加和扩展的安全性，在网络段之间是需要的。它也能保护企业内部网和外部网连接的附加安全，也管理分支办公室站点连接到总部或者 Internet。

Cisco IOS 防火墙入侵检测能识别 59 种常见的攻击，使用特征来探测网络流量滥用。入侵检测特征在 Cisco IOS 防火墙入侵检测特性集的新版本中选择了宽泛的入侵检测特征穿越区。这些特征能有效阻止对安全构成危险的大多数普通网络攻击和攫取信息的扫描。

当然，CBAC 也有许多缺陷：它不能提供智能地过滤所有协议，它仅能在制订的规则下工作。如果没有指定一个协议给 CBAC，那么已存在的 ACL 将决定协议是否被过滤，而不会给未指定的协议开临时通道。CBAC 不会保护源于受保护网络的攻击，除非流量穿越



一个有 Cisco IOS 防火墙特性的路由器。CBAC 只检测和保护穿过防火墙的攻击流量。

2. 配置 CBAC

下面简要介绍在基于 Cisco IOS 防火墙上配置 CBAC 的过程。

❶ 定义一个 ACL，并将其应用到某个接口上。

```
Router(config)# ip access-list extended banedonkey
Router(config-ext-nacl)# deny tcp any any range 4661 4662
Router(config-ext-nacl)# deny tcp any any range 4242 4243
Router(config-ext-nacl)# deny udp any any eq 4665
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group banedonkey in
Router(config-if)# ip access-group banedonkey out
```

❷ 定义一个 CBAC 列表。

```
Router(config)# ip inspect name CBAC smtp audit-trail on //打开审计功能
Router(config)# ip inspect name CBAC ftp   alert on  //打开报警功能
Router(config)# ip inspect name CBAC http
Router(config)# ip inspect name CBAC realaudio
Router(config)# ip inspect name CBAC tcp
Router(config)# ip inspect name CBAC udp
Router(config)# ip inspect name CBAC icmp
```

❸ 在接口上应用 CBAC 规则。

```
Router(config-if)# ip inspect CBAC in
```

3. 应对攻击

通常，在网络中大量的病毒是通过 Java 小程序进行传播的，因此有必要对不可信区域发送来的 Java 小程序进行过滤。过滤方法如下。

❶ 定义一个 ACL，用于放行可信区域 Java 小程序。

```
Router(config)# ip access-list standard banjava
Router(config-ext-nacl)# deny 46.1.0.0 0.0.255.255   //排除可信区域
Router(config-ext-nacl)# permit any
Router(config-ext-nacl)# exit
```

❷ 配置 CBAC 阻隔 Java 小程序。

```
Router(config)# ip inspect name deny-java http java-list banjava
Router(config)# interface ethernet0
Router(config-if)# ip inspect deny-java out
```

❸ 为了交换机、路由器的安全，还可以对 TCP、UDP 进行限制。

```
Router(config)# ip inspect tcp synwait-time 15
Router(config)# ip inspect tcp idle-time 120
Router(config)# ip inspect udp idle-time 20
```

❹ 在一些特殊情况下，还需要对 URL 进行过滤。URL 过滤可以使用如下方式。

```
Router(config)# ip inspect name url-filter http urlfilter  //创建URL过滤服务器
Router(config)# ip urlfilter server vendor websense 46.1.23.1  //指定内容过
滤服务器
```

```
Router(config)# ip urlfilter cache 7000              //URL缓存大小
Router(config)# ip urlfilter max-request 1500        //URL最大请求数
Router(config)# ip urlfilter max-resp-pack 300       //URL最大回复数
Router(config)# ip urlfilter exclusive-domain permit .cisco.com
Router(config)# ip urlfilter exclusive-domain deny .sex.com
//排除域，直接通过cisco.com的流量，并禁止sex.com的非法流量
Router(config)# ip urlfilter audit-trail             //为URL过滤服务器创建审计
Router(config)# ip urlfilter alert                   //创建URL报警
Router(config)# ip urlfilter urlf-server-log         //创建URL过滤服务器日志
Router(config)# interface Ethernet1
Router(config-if)# ip inspect url-filter out         //应用CBAC
```

8.2.3 基于网络的应用识别

基于网络的应用识别(Network-Based Application Recognition，NBAR)是一种动态的、能在第四层至第七层识别协议的技术，它不但能像普通 ACL 那样控制静态的、简单的网络应用协议 TCP/UDP 的端口号(例如，我们熟知的 Web 应用使用的 TCP 80 端口)，也能做到控制一般 ACL 不能做到的使用动态端口的那些协议，例如 VoIP 使用的 H.323、SIP 等。

在使用 NBAR 的时候，首先要启用 CEF 特性，并使用数据包描述语言模块(PDLM)从路由器的闪存里加载，用于在不使用新的 Cisco IOS 软件，或重启路由器的情况下对新的协议或应用程序进行识别。

应用 NBAR 时，不能在快速以太网信道、使用了隧道或加密技术的接口、SVI、拨号接口和多链路 PPP(MLP)这些接口上启用，并且存在如下限制。

- 不支持多于 24 个的并发 URL、HOST 或 MINE 的匹配类型。
- 不支持超过 400 B 的 URL 匹配。
- 不支持非 IP 流量。
- 不支持组播或其他非 CEF 的交换模式。
- 不支持被分片的数据包。
- 不支持源自或去往运行 NBAR 的路由器的 IP 流。

1. NBAR 的配置过程

下面简要介绍在基于 Cisco IOS 防火墙上配置 NBAR 的过程。

❶ 启用路由器的 CEF 特性。

```
Router(config)#ip cef
```

❷ 通过定义类映射把流量进行分类，并设置相应的匹配规则。

```
Router(config)#class-map [match-all|match-any] {map-name}
Router(config-cmap)#match protocol {protocol}
```

❸ 设置策略映射，并调用上一步配置的类映射。

```
Router(config)#policy-map {policy-name}
Router(config-pmap)#class {class-map}
Router(config-pmap-c)#drop
```

❹ 将策略应用到接口。

```
Router(config)#interface FastEthernet 1/x
Router(config-if)#service-policy {input|output} {policy-map}
```

❺ 可以使用如下命令验证 NBAR 配置。

```
Router#show class-map [map-name]         // 查看流量分类信息
Router#show policy-map [policy-name]     //查看策略映射
Router#show policy-map interface [interface]   //查看接口的策略映射信息
Router#show ip nbar pdlm                 //显示NBAR所使用的PDLM
Router#show ip nbar port-map             //显示NBAR使用的协议到端口号的映射信息
```

2. 利用 NBAR 进行流量控制

NBAR 可以方便地进行一些应用的过滤，最常见就是一些基于 P2P 应用的过滤。BT/eDonkey 这类 P2P 软件使用非常方便，就像一个浏览器插件，很适合新发布的热门下载。其特点简单地说就是下载的人越多，速度越快。由于 BT/eDonkey 大量的使用会造成网络带宽被尽情消耗，导致一些企业和单位的关键业务不能正常运行，所以有必要对 BT/eDonkey 流量进行控制。

要实现对 BT/eDonkey 流量的控制，就要在 Cisco 路由器上实现对 PDLM(Packet Description Language Module，数据包描述语言模块)的支持。PDLM 是一种对网络高层应用的协议层的描述，例如协议类型、服务端口号等。它的优势是让 NBAR 适应很多已有的网络应用，如 HTTP、DNS、FTP、VoIP 等，同时它还可以通过定义来使 NBAR 支持许多新兴的网络应用。PDLM 可以在 Cisco 的网站上下载，利用 PDLM 可以限制一些网络上的恶意流量。

下面介绍利用 PDLM 实现对 BT/eDonkey 流量的控制。

❶ 加载相应的 PDLM 模块。

```
Router(config)# ip nbar pdlm bittorrent.pdlm
Router(config)# ip nbar pdlm edonkey.pdlm
```

❷ 定义类映射。

```
Router(config)#class-map match-all bittorrent
Router(config-cmap)#match protocol bittorrent
Router(config)#class-map match-all edonkey
Router(config-cmap)#match protocol edonkey
```

❸ 定义策略映射。

```
Router(config)#policy-map btedonkey
Router(config-pmap)# class bittorrent
Router(config-pmap-c)#drop
Router(config-pmap)# class edonkey
Router(config-pmap-c)#drop
```

//除 drop 策略外，IOS 还支持对应用进行限速

```
Router(config-pmap-c)# police cir 240000
Router(config-pmap-c)# conform-action transmit
Router(config-pmap-c)# exceed-action drop
```

❹ 将策略应用到网络接口。

```
Router(config)#interface FastEthernet 1/x
Router(config-if)# service-policy input btedonkey
Router(config-if)# service-policy output btedonkey
```

3. 利用 NBAR 过滤蠕虫病毒

在某些情况下，NBAR 也可以用于对 Nimda 和 Red Code 这类蠕虫病毒的过滤。其配置方法如下。

```
ip cef
!
class-map match-all DENY-ATTACK
match protocol http url "*.ida*"
match protocol http url "*cmd.exe*"
match protocol http url "*root.exe*"
match protocol http url "*readme.eml*"
!
policy-map antiworm class DENY-ATTACK drop
interface Serial0
ip address 10.0.0.1 255.255.255.252
service-policy input antiworm
```

8.3 Cisco PIX/ASA 防火墙

在 Internet 上大量使用的防火墙产品就是 Cisco 的 PIX 防火墙，国内众多银行、证券机构、政府机构也大量使用该产品。

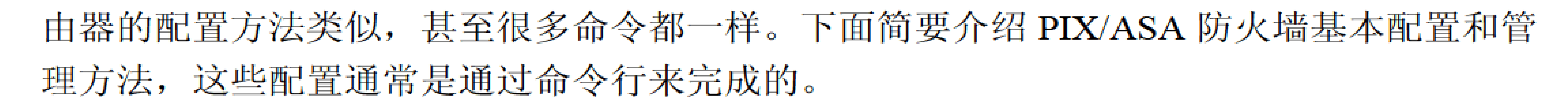
但是黑客们日益聚焦于混合型的威胁，结合各种有害代码来探测和攻击系统漏洞。这些混合攻击分别绕过现有的安全结点，如独立的 VPN、防火墙和防毒产品，形成各种形态、持续的攻击流。黑客自动工具、混合攻击以及蠕虫和木马病毒增加了数据曝光的可能性。脆弱点、配置错误和缺乏管理等问题更使实现安全的难度增加。威胁的形态表现为病毒、蠕虫、木马、灰色件、间谍件、垃圾邮件、配置错误、应用程序脆弱点、自动的黑客工具和脚本、拒绝服务、缓冲溢出、Cookie 中毒等。威胁的另一特点是新漏洞攻击产生的速度快，即称为“零小时”(0 hour)或“零日”(0 day)新的未知的攻击。另外，社会工程陷阱型的攻击，包括间谍软件、网络欺诈、基于邮件的攻击和恶意 Web 站点、Web 重定向等，伪装为合法应用和邮件信息欺骗用户的威胁日益增多。

2005 年 5 月，Cisco 推出了一个新的产品——适应性安全产品(Adaptive Security Appliance，ASA)。ASA 是 Cisco 系列中全新的防火墙和反恶意软件安全工具，它包括 Firewall、IPS、Anti-X 和 VPN 四种功能。同时，IDC 提出将防病毒、入侵检测和防火墙安全设备命名为统一威胁管理(United Threat Management，UTM)设备。

而 ASA 恰好针对这些不同类型的攻击提供了防护。加装一个内容安全及控制安全服务模块(Content Security Control and Security Service Module，CSC-SSM)后，它比一台 UTM 设备具有更高的安全性。

8.3.1 PIX/ASA 防火墙基本配置

作为 Cisco 公司生产的网络安全产品，PIX/ASA 防火墙的配置方法与 Cisco 交换机/路



由器的配置方法类似，甚至很多命令都一样。下面简要介绍 PIX/ASA 防火墙基本配置和管理方法，这些配置通常是通过命令行来完成的。

1. 检查 License

对于一台 PIX 防火墙，需要检查它的许可协议是否可用。检查方法如下。

❶ 通过 show version 命令，查看序列号和激活码。

```
pixfirewall#  show version
Cisco PIX Security Appliance Software Version 8.0(2)
Device Manager Version 6.0(2)

Compiled on Fri 15-Jun-07 18:25 by builders
System image file is "flash:/pix802.bin"
Config file at boot was "startup-config"

pixfirewall up 10 mins 43 secs

Hardware:   PIX-525,  1024 MB RAM,  CPU Pentium III  1000 MHz
Flash E28F128J3 @ 0xfff00000,  16MB
BIOS Flash AM29F400B @ 0xfffd8000,  32KB

 0: Ext: Ethernet0          : address is 0010.7800.0001,  irq 9
 1: Ext: Ethernet1          : address is 0010.7800.0002,  irq 11
 2: Ext: Ethernet2          : address is 0010.7800.0003,  irq 11

Licensed features for this platform:
Maximum Physical Interfaces     : 10
Maximum VLANs                  : 100
Inside Hosts                   : Unlimited
Failover                       : Active/Active
VPN-DES                        : Enabled
VPN-3DES-AES                   : Enabled
Cut-through Proxy              : Enabled
Guards                         : Enabled
URL Filtering                  : Enabled
Security Contexts              : 2
GTP/GPRS                       : Disabled
VPN Peers                    : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: *********
Running Activation Key: *********************************
Configuration has not been modified since last system restart.
```

❷ 如果尚未激活，则需使用如下命令输入激活码激活。

```
pixfirewall# activation-key ?
  <0x0-0xffffffff>  Enter four-or-five-tuple activation-key
  noconfirm         Do not prompt for confirmation
```

2. 基本连通性配置

图 8-11 所示为 Sadness 公司边界防火墙配置示意图，在建立一系列安全策略前，需要将网络连接通畅。

下面是基本连通性的配置过程：

❶ 根据图 8-11 所示的拓扑，配置每个网络接口的 IP 地址、速率、双工模式、别名，并定义相应的安全等级。

```
Firewall(config)# interface  gigabitethernet0
Firewall(config-if)# speed auto
Firewall(config-if)# duplex auto
Firewall(config-if)# nameif inside
Firewall(config-if)# security-level 100
Firewall(config-if)# ip address 192.168.1.0   255.255.255.0
Firewall(config)# interface  gigabitethernet1
Firewall(config-if)# speed auto
Firewall(config-if)# duplex auto
Firewall(config-if)# nameif outside
Firewall(config-if)# security-level 0
Firewall(config-if)# ip address 192.168.2.0   255.255.255.0
Firewall(config)# interface  gigabitethernet2
Firewall(config-if)# speed auto
Firewall(config-if)# duplex auto
Firewall(config-if)# nameif dmz
Firewall(config-if)# security-level 50
Firewall(config-if)# ip address 192.168.3.0   255.255.255.0
```

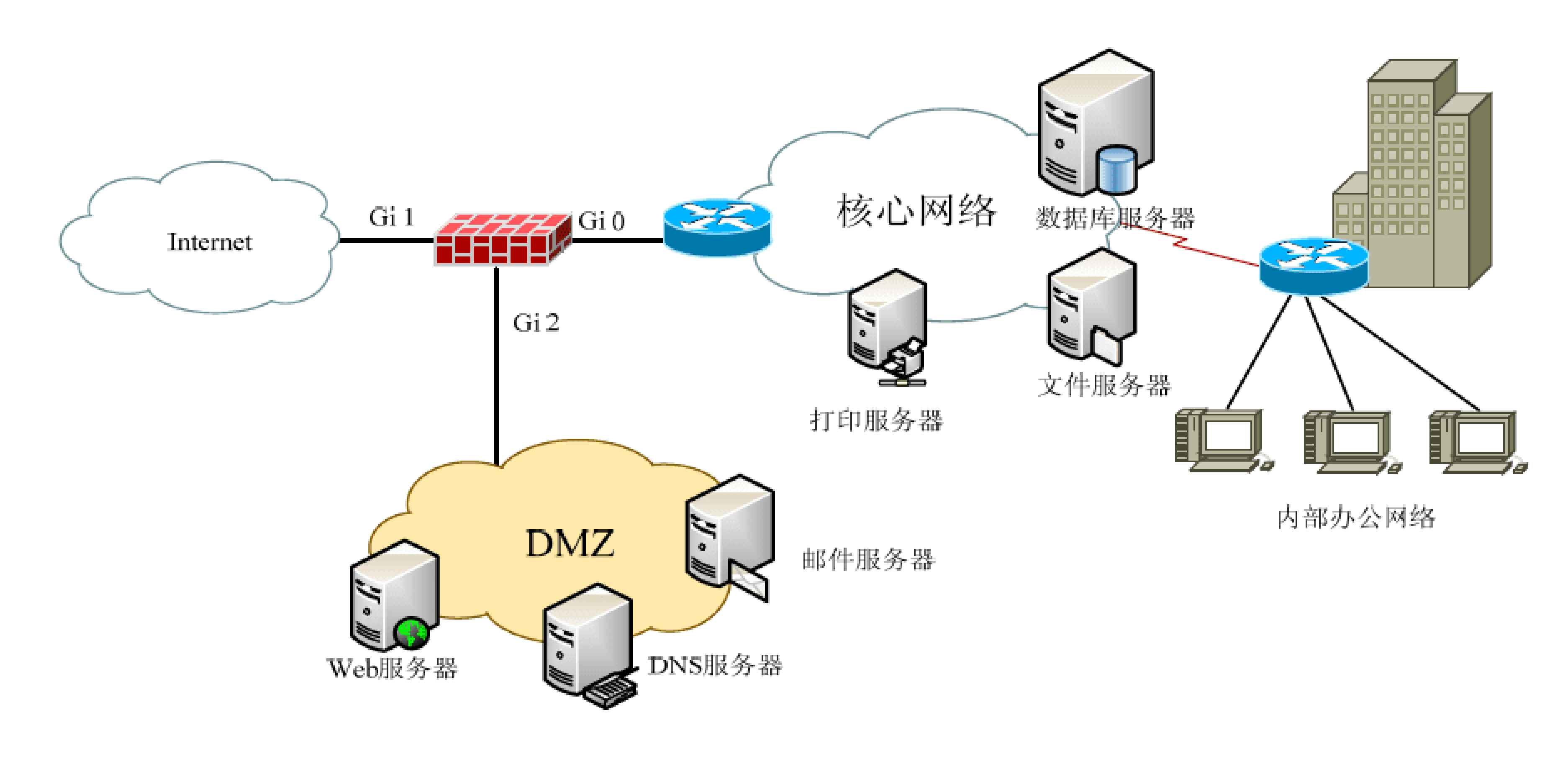


图 8-11　Sadness 公司边界防火墙

❷ 为了保证数据包能正确转发，还需要配置路由表。如果网络结构简单，可以使用下面的方法配置静态路由。

```
Firewall(config)# route if_name 0.0.0.0  0.0.0.0  gateway_ip [metric]
```

❸ PIX 也可以配置动态路由协议，和 IOS 路由器的配置方法类似。下面是配置 OSPF 动态路由协议的例子。

```
Firewall(config)# router ospf 1
Firewall(config-router)# router-id  192.168.1.1
Firewall(config-router)# network  192.168.1.0 255.255.255.0 area 0
Firewall(config-router)# network  192.168.0.0 255.255.0.0 area 100
Firewall(config-router)# area 0  authentication message-digest
Firewall(config-router)# area 0 filter-  list prefix InsideFilter in
Firewall(config-router)# area 100  authentication message-digest
```

```
Firewall(config-router)# exit
Firewall(config)# interface  gigabitethernet1
Firewall(config-if)# ospf message-digest-key 1 md5 cisco
Firewall(config-if)# interface  gigabitethernet0
Firewall(config-if)# ospf message-digest-key 1 md5 cisco
Firewall(config-if)# exit
```

❹ 在某些时候，外部全局地址有限，需要配置 NAT 地址转换。其配置模板如下。

```
Firewall(config)#  global  (outside)  1  46.1.1.10-46.1.1.60  netmask
255.255.255.128
Firewall(config)# global (outside) 1 46.1.1.61
Firewall(config)# nat (inside) 1 10.16.0.0 255.255.0.0 0 0
Firewall(config)#  global  (outside)  2  46.1.1.65-46.1.1.125  netmask
255.255.255.128
Firewall(config)# global (outside) 2 46.1.1.126
Firewall(config)# nat (inside) 2 10.17.0.0 255.255.0.0 0 0
Firewall(config)# global (outside) 3 interface
Firewall(config)# nat (inside) 3 access-list nat_0 0 0 0
Firewall(config)#  access-list  acl_no_nat  permit  ip  host  10.16.1.1
192.168.23.0  255.255.255.0
Firewall(config)# nat (inside) 0 access-list acl_no_nat
Firewall(config)# access-list acl_inside permit ip 10.16.0.0 255.240.0.0 any
Firewall(config)# access-list acl_inside permit ip 192.168.12.0 255.255.255.0
any
Firewall(config)# access-list acl_inside deny ip any any
Firewall(config)# access-group acl_inside in interface inside
```

❺ 为了提高安全性，还可以配置 uRPF。

```
Firewall# show ip verify statistics [interface if_name]
```

❻ 可以通过 show route 命令查看路由表，验证路由配置是否正确。

```
Firewall# show route
S    0.0.0.0 0.0.0.0 [1/0] via 10.74.3.3,  outside
C    10.74.3.3 255.255.255.128 is directly connected,  outside
O    192.168.3.0 255.255.255.0 [1/0] via 192.168.4.4,  inside
C    192.168.4.0 255.255.255.0 is directly connected,  inside
Firewall#
```

3. 配置 PIX/ASA 的远程管理方式

通常，PIX/ASA 可以通过 SSH、Telnet 以及 ASDM/PDM(自适应安全设备管理器/PIX 设备管理器)的方式进行远程管理。配置远程管理的方法如下。

❶ 创建登录用户及密码。通常 PIX/ASA 除了支持本地用户/密码数据库以外，还支持基于 AAA 的登录方式。

```
Firewall(config)# aaa-server sadnessRadius protocol radius
Firewall(config)# aaa-server sadnessRadius (inside) host 10.0.98.10 key
Cisco
Firewall(config)# aaa-server sadnessRadius (inside) host 10.0.98.11 key
Cisco
Firewall(config)# aaa-server sadnessRadius (inside) host 10.0.98.12 key
Cisco
Firewall(config)# aaa-server sadnessRadius (inside) host 10.0.98.13 key
Cisco
Firewall(config)# aaa-server sadnessRadius (inside) host 10.0.98.14 key
```

```
Cisco
Firewall(config)# aaa authentication serial console sadnessRadius LOCAL
Firewall(config)# aaa authentication telnet console sadnessRadius LOCAL
Firewall(config)# aaa authentication ssh console sadnessRadius LOCAL
Firewall(config)# aaa authentication http console sadnessRadius LOCAL
Firewall(config)# aaa authentication enable console sadnessRadius LOCAL
Firewall(config)# username admin password AdminPW privilege 15
```

❷ 配置 SSH 登录。例如，需要从 IP 为 192.168.1.4 的主机通过 SSH 方式访问 inside 接口。

```
pixfirewall(config)# hostname SadnessFW                    //配置域名
SadnessFW(config)# domain-name sadness.net                 //配置主机名
SadnessFW(config)# crypto key generate rsa modulus 1024  //生成密钥
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
SadnessFW(config)# ssh 192.168.1.4 255.255.255.255 inside//配置SSH接入控制
```

❸ 配置 Telnet 登录。例如，要允许连接在 inside 接口上、IP 地址为 192.168.1.3 的主机通过 Telnet 访问防火墙。

```
Firewall(config)#telent 192.168.1.3 255.255.255.255 inside
```

❹ 如果希望能够通过图形化界面来管理 PIX/ASA，则需要配置 ASDM/PDM 登录，例如需要从 IP 为 192.168.1.0/24 网络的主机通过 ASDM 访问 inside 接口。对于使用 ASDM 管理 PIX/ASA 将在下一节中介绍。

```
SadnessFW(config)# http server enable
SadnessFW(config)# http 192.168.1.0 255.255.255.0 inside
```

4. 配置故障倒换

通常，PIX/ASA 部署方式为串行接入网络，即一端连接外部网络，另一端连接内部网络。如果在区域分割的三角方式中，还有一端连接 DMZ 主机，当 PIX/ASA 出现故障后，这样的拓扑结构非常容易造成单点失效故障。因此有必要对 PIX 进行热备份保护，即配置 PIX/ASA 故障倒换，其连接方式如图 8-12 所示。

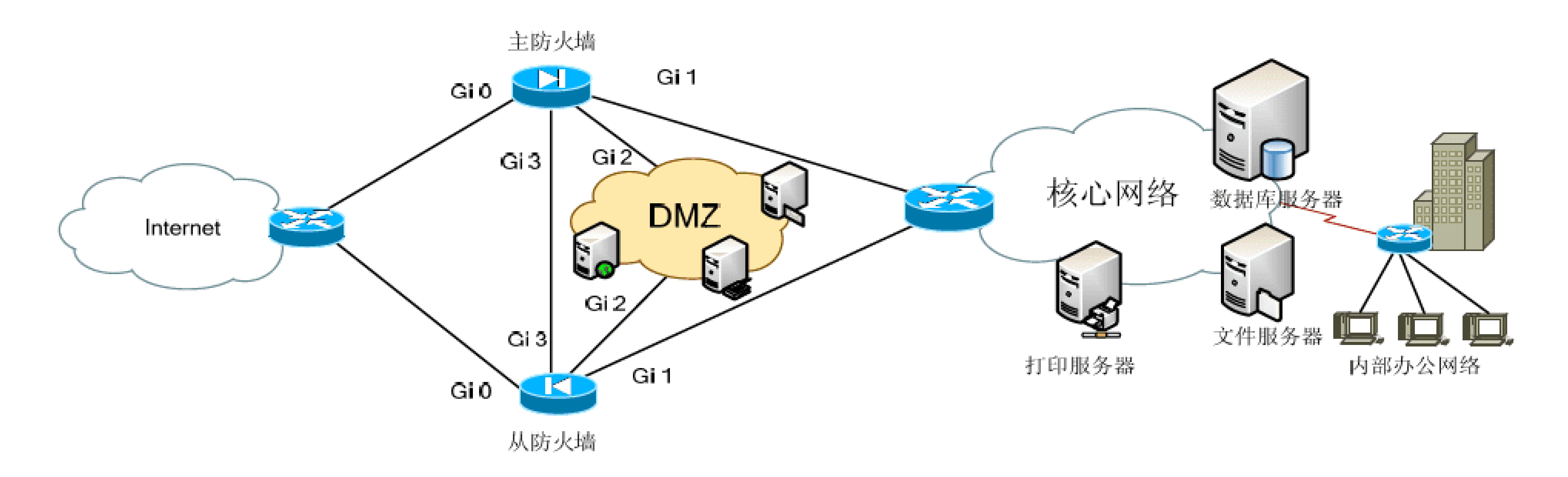


图 8-12 故障倒换拓扑结构

配置故障倒换的操作步骤如下。

❶ 按照下列方式配置主(Primary)防火墙。

```
interface GigabiteEthernet0
speed 100
```

```
nameif outside
security-level 0
ip address 10.131.0.1 255.255.255.0 standby 10.131.0.2
!
interface GigabiteEthernet1
speed 100
nameif inside
security-level 100
ip address 10.0.0.1 255.255.255.0 standby 10.0.0.2
!
interface GigabiteEthernet2
speed 100
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
failover lan interface lanfail GigabiteEthernet3
failover key *****
failover interface ip lanfail 172.16.12.1 255.255.255.0 standby 172.16.12.2
failover lan unit primary
failover lan enable
failover
```

❷ 按照下列方式配置从(Secondary)防火墙。

```
failover lan interface lanfail GigabiteEthernet3
failover key sadnesswork
failover interface ip lanfail 172.16.12.1 255.255.255.0 standby 172.16.12.2
failover lan unit secondary
failover lan enable
failover
```

❸ 当两台防火墙发生意外(例如同时断电)时，如果没有防火墙的硬件备份的话，管理员将面临巨大的心理压力。假如把防火墙配置成透明模式(可称为伪网桥)，就无需更改网络架构，即使是防火墙不能工作了，要做的仅仅是拔出网线，把网线直接插入路由器的内部接口，网络就可以正常工作了，然后就有时间慢慢恢复发生故障的防火墙。

```
Firewall(config)#firewall transparent
Firewall(config)# interface  Gigabitethernet0
Firewall(config-if)# speed auto
Firewall(config-if)# duplex auto
Firewall(config-if)# nameif inside
Firewall(config-if)# security-level 100
Firewall(config)# interface  Gigabitethernet1
Firewall(config-if)# speed auto
Firewall(config-if)# duplex auto
Firewall(config-if)# nameif outside
Firewall(config-if)# security-level 0
```

8.3.2　利用 ASDM 配置 PIX/ASA 防火墙

为了简化 PIX/ASA 防火墙的配置和管理，Cisco 提供了 ASDM。ASDM 基于图形化配置和管理 PIX/ASA 防火墙，这比使用命令行方式配置 PIX/ASA 防火墙要简单得多。下面简要介绍 ASDM 的安装方法及主要配置功能。

1. 安装 ASDM

由于 Cisco PIX 6.x 以下版本的软件不支持 ASDM，因此安装 ASDM 之前，需要将 PIX 升级到 7.0。可以通过 show version 命令来查看软件的版本和 PIX 的型号。在升级时需要注意，如果使用的是 PIX 515 或者 515e 设备，需要升级内存才能安装 PIX 7.0，这是因为 PIX 515/515e 系列产品总内存容量为 32MB，而 PIX 7.0 和 ASDM 需要 64MB 的内存。

下面简要介绍 ASDM 的安装过程。

❶ 从 Cisco 网站下载 ASDM 图像，将其存放在网络中某台 TFTP 服务器上。在本例中使用的是 ASDM 的 5.02 版，文件名为 asdm502.bin。

❷ 通过 Consol 接口或远程登录到 PIX/ASA 防火墙，进入防火墙的特权模式。

```
SadnessFW > enable
SadnessFW #
```

❸ 将 TFTP 服务器中的 ASDM 图像复制到 PIX 防火墙的 Flash 中。

```
SadnessFW # copy tftp flash
Address or name of remote host [x.x.x.x]?  192.168.1.100<CR>
Source file name [cdisk]? asdm502.bin <CR>        //输入ASDM图像的文件名
Destination file name [asdm502.bin]?<CR>
```

❹ 告诉 PIX 软件 ASDM 存储的位置。

```
SadnessFW #configure termina
SadnessFW (config)# asdm image flash:asdm502.bin
```

❺ 启动 HTTP/HTTPS 服务器，并设置允许通过 ASDM 访问防火墙的主机的位置。例如需要从 IP 为 192.168.1.0/24 网络的主机通过 ASDM 访问 inside 接口。

```
SadnessFW(config)# http server enable
SadnessFW(config)# http 192.168.1.0 255.255.255.0 inside
```

❻ 配置完成后，保存上述配置。

```
SadnessFW (config)# write memory
```

❼ 保存配置后，可以通过 ASDM 软件或者浏览器访问 “https://<firewall-ip-address>” 来配置或管理 PIX/ASA 防火墙，如图 8-13 所示。



图 8-13　通过 ASDM 管理防火墙

❽ 输入用户名和密码登录后，便可以进入 ASDM 管理界面，如图 8-14 所示。

图 8-14　ASDM 管理界面

2. 配置日志

日志服务可以记录所有对防火墙的配置行为，当防火墙被非法配置后，可以向管理员发送警报并进行追踪。下面是利用 ASDM 来配置 PIX/ASA 防火墙日志的过程。

❶ 打开 ASDM 管理界面后，选择 Configuration→Device Management →Logging→Logging Setup 结点，选中 Enable logging 复选框，开启日志服务功能用于监控 PIX/ASA 防火墙，如图 8-15 所示。

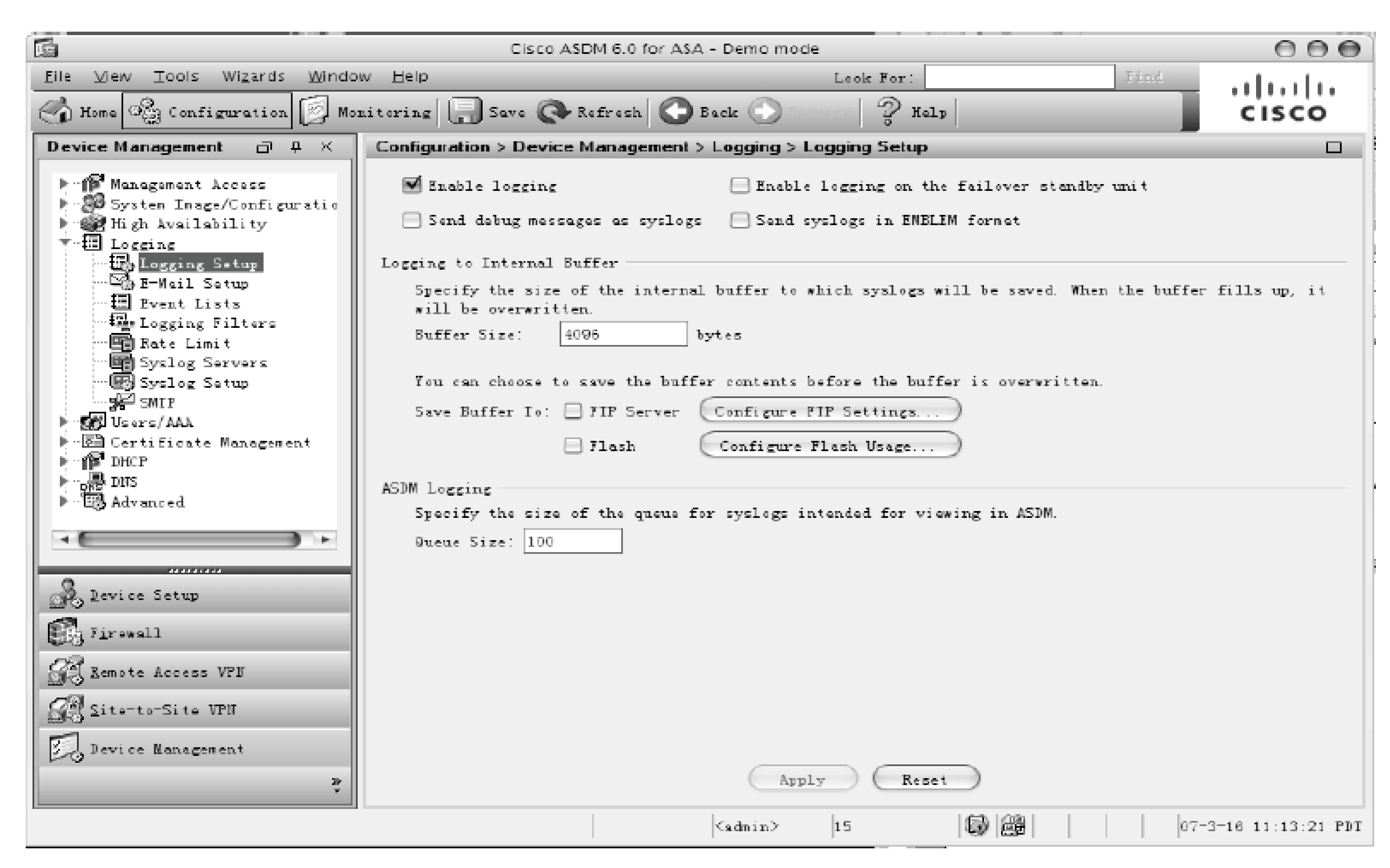


图 8-15　开启日志服务功能

❷ 单击 Logging Filters 结点，在右侧的窗格中选择 ASDM 一行，并将其 Filter on severity 下拉列表框设置为 Warnings，如图 8-16 所示。

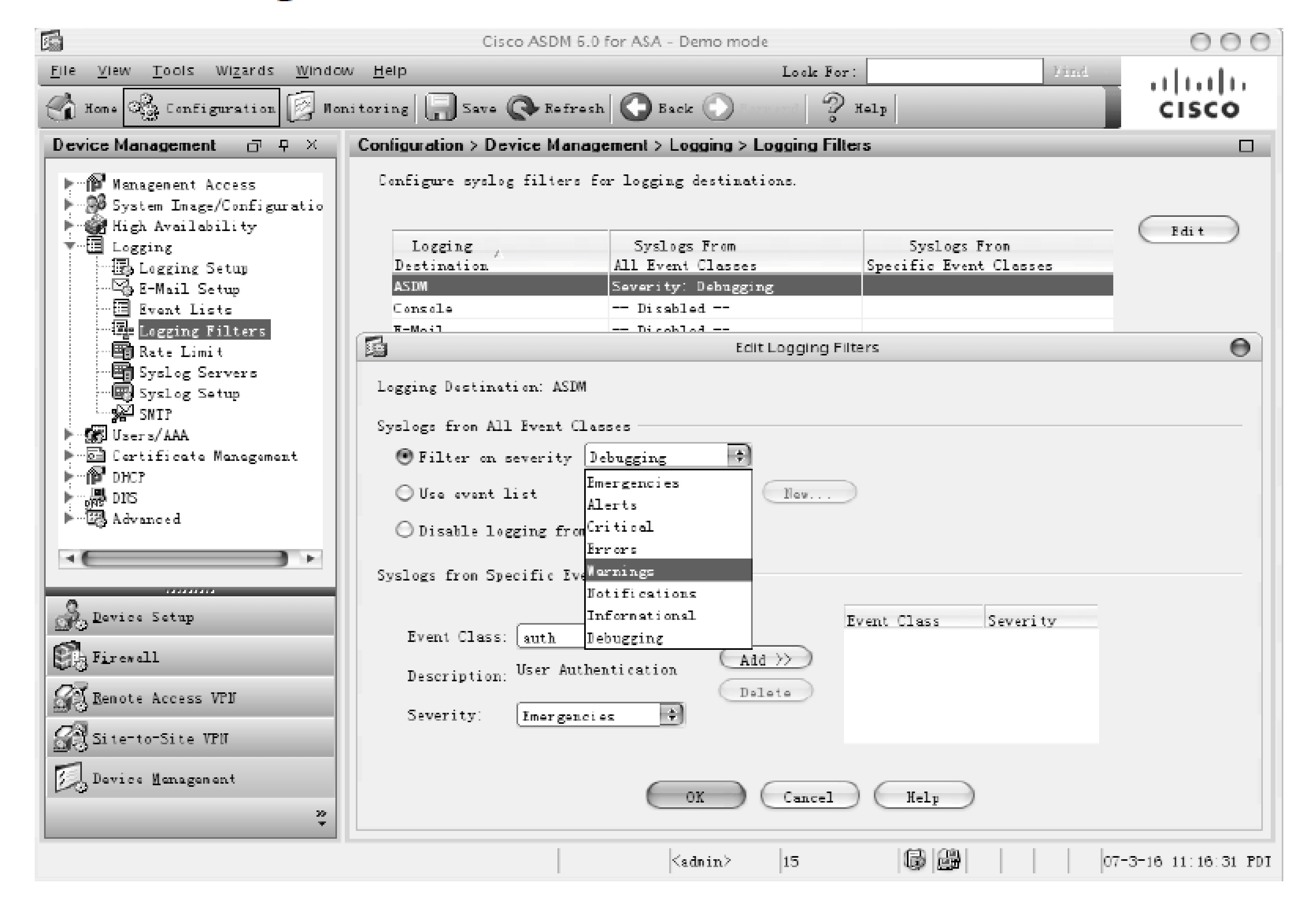


图 8-16　配置日志服务功能

3. 设置网络连接

ASDM 提供了基于图形化的接口 IP 地址、接口名称、安全等级等定义方式，并且路由协议、故障倒换等也可以通过 ASDM 定义。其操作方法如下。

❶ 选择 Configuration→ Device Setup →Interfacses 结点，可以配置接口 IP 地址、安全等级等参数，如图 8-17 所示。

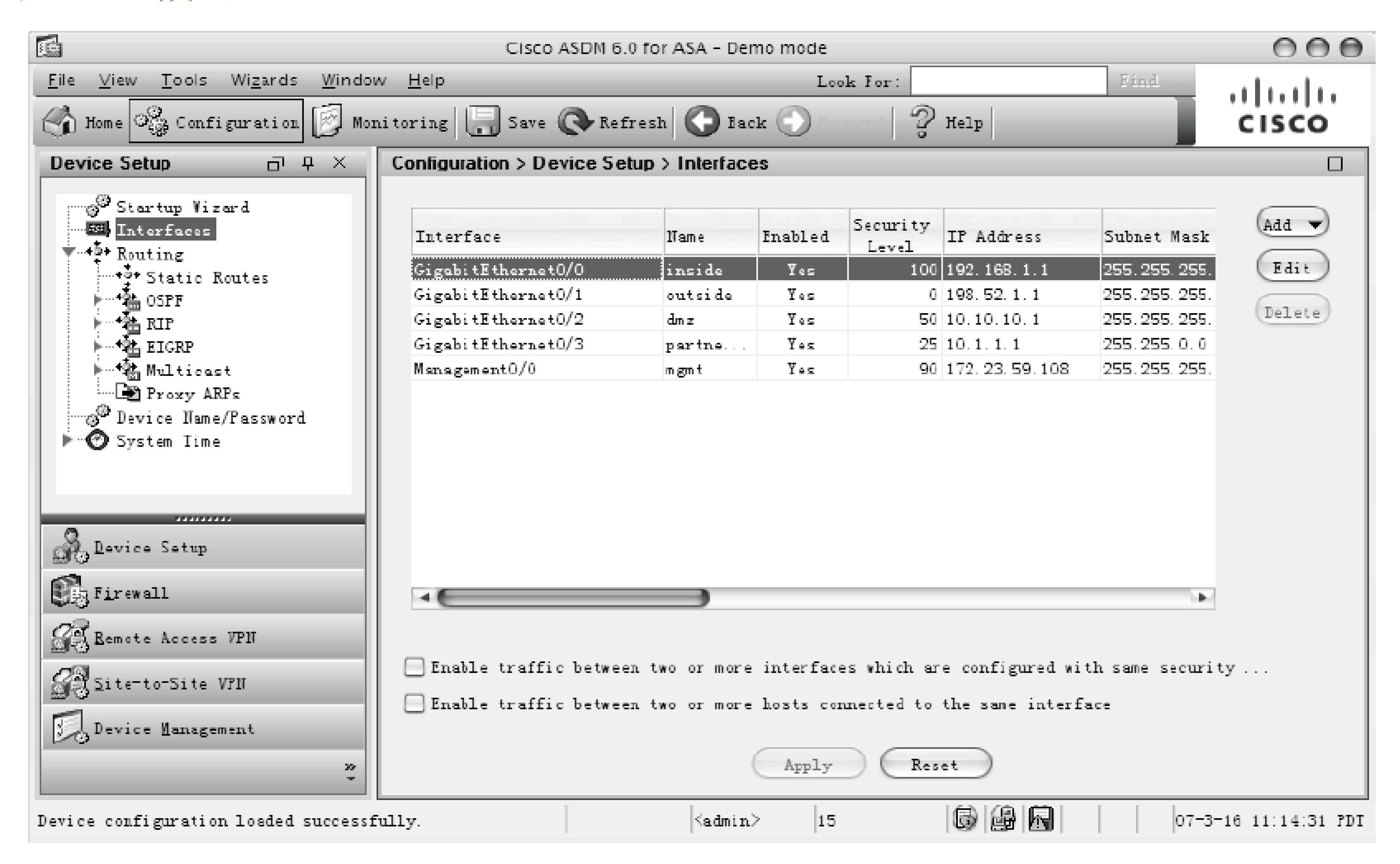


图 8-17　配置接口 IP 地址

❷ 选择 Configuration→ Device Setup →Routing 结点，可以配置多种路由协议，如图 8-18 所示。

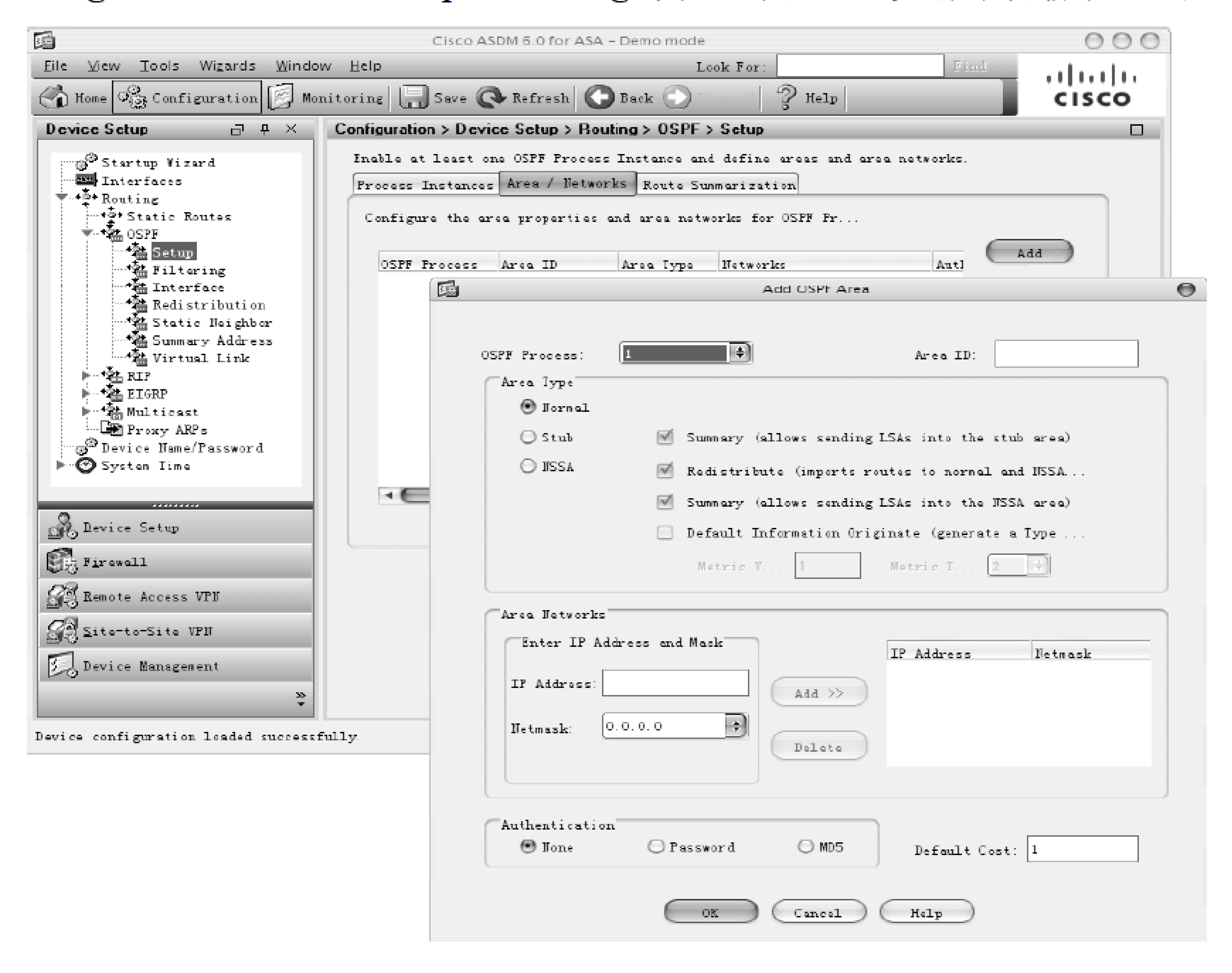


图 8-18　配置路由协议

❸ 选择 Configuration→ Device Management →High Availability 结点，可以配置故障倒换属性，如图 8-19 所示。



图 8-19　配置故障倒换

4．配置安全访问策略

通常，我们将 Web 服务器、DNS 服务器以及邮件服务器放入 DMZ 区域中。因此需要定义一些策略，让它们能够通过一些方式被内部网络和外部网络访问。

例如，在图 8-20 中，需要允许以下流量的访问。

✧ 允许内部网络到 DMZ 区域的 DNS 服务器、E-mail 服务器、Web 服务器的访问；
✧ 允许 DMZ 区域的 DNS 服务器、E-mail 服务器到外部网络的访问；
✧ 允许外部网络访问 DMZ 区域的服务器。

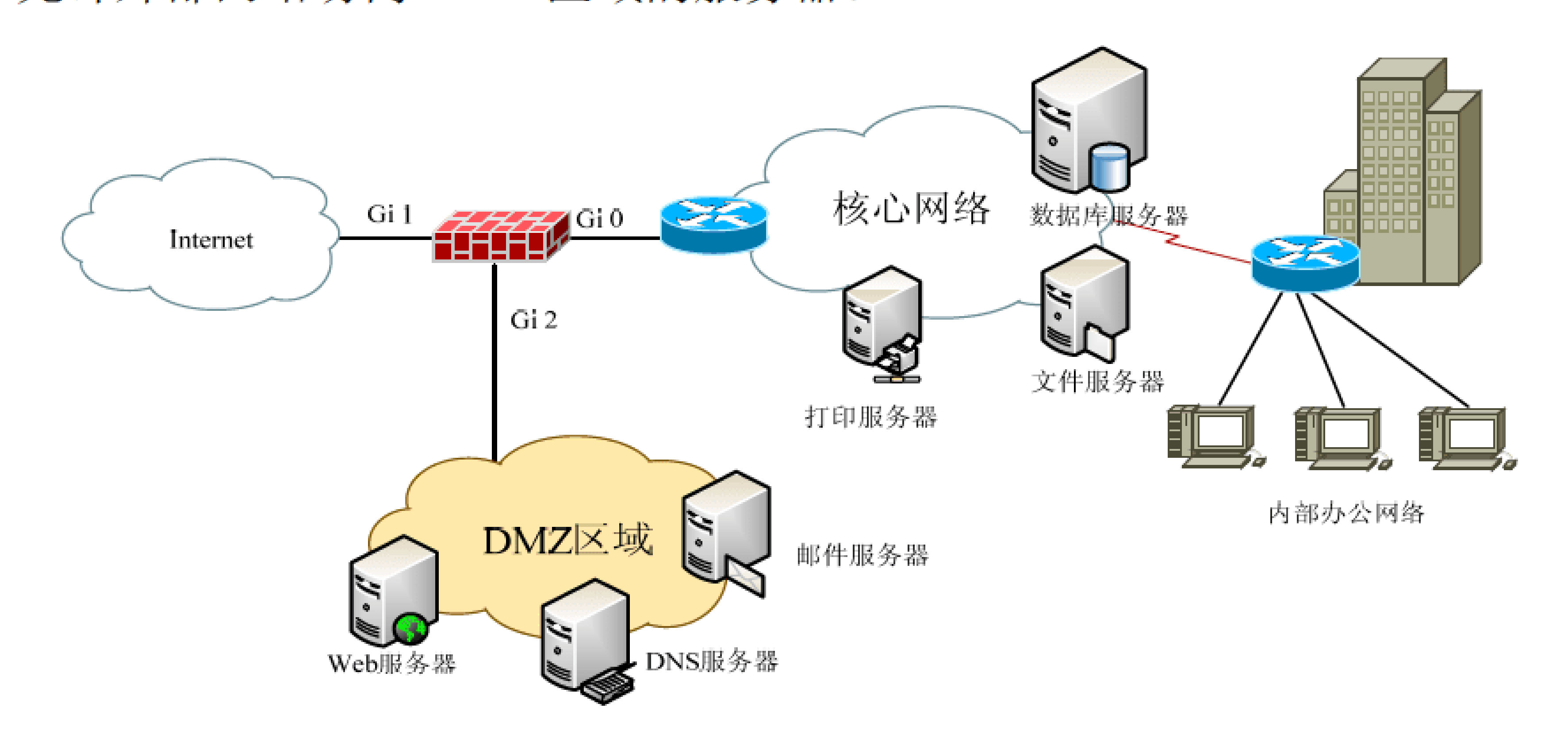


图 8-20　安全访问策略

要实现上述目标，可以按以下方式来配置。

❶ 定义端口组。选择 Configuration→ Firewall→ Objects→Service Groups 结点，可以配置一系列服务所使用的端口构成的端口组，如图 8-21 所示。

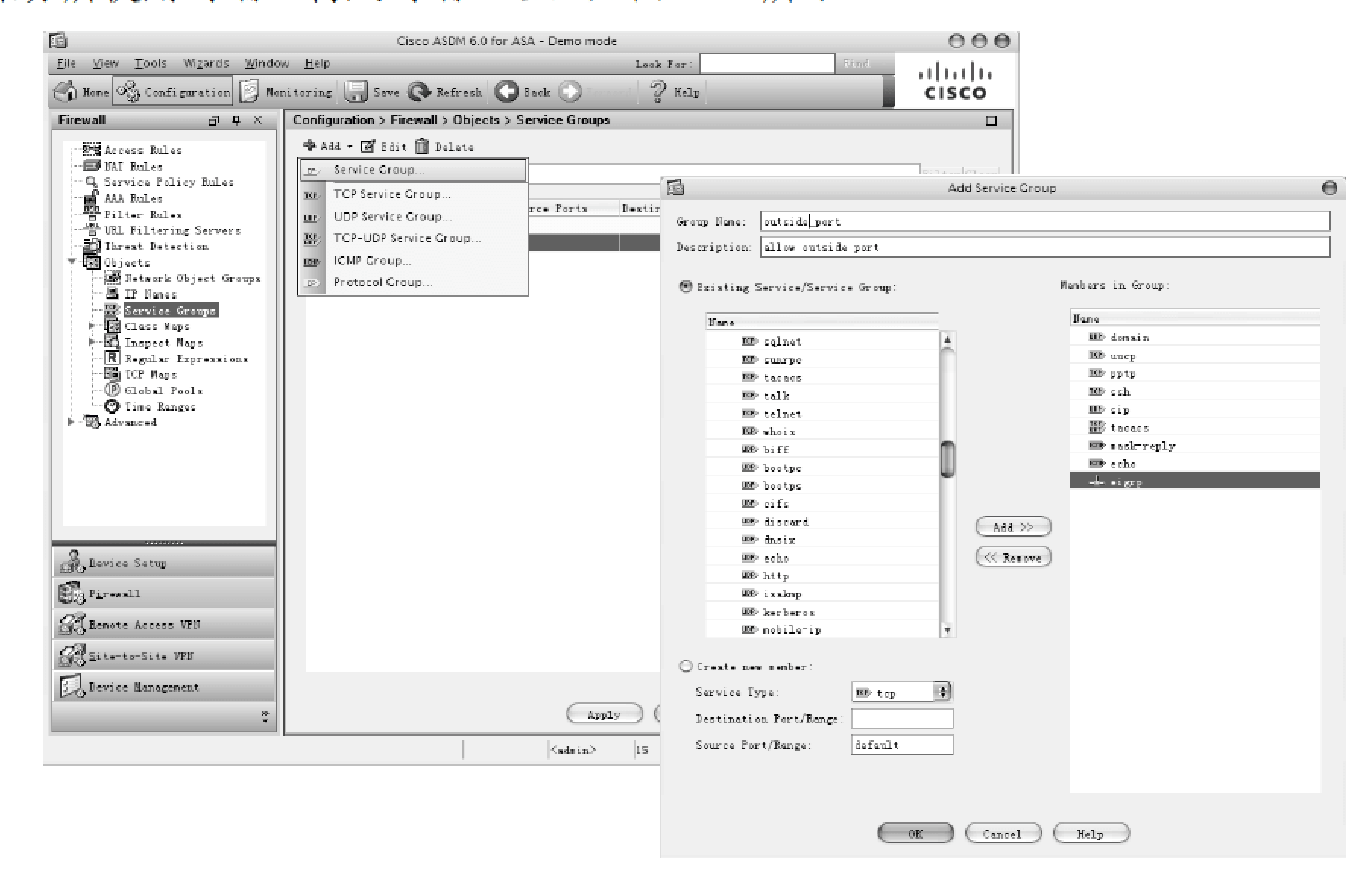


图 8-21　配置服务端口组

❷ 选择 Configuration→Firewall →Access Rules 结点，并选择 Add Access Rule 命令，在打开的对话框中可以配置访问规则，并且可以在 Service 选项中关联前一步创建的端口组，如图 8-22 所示。

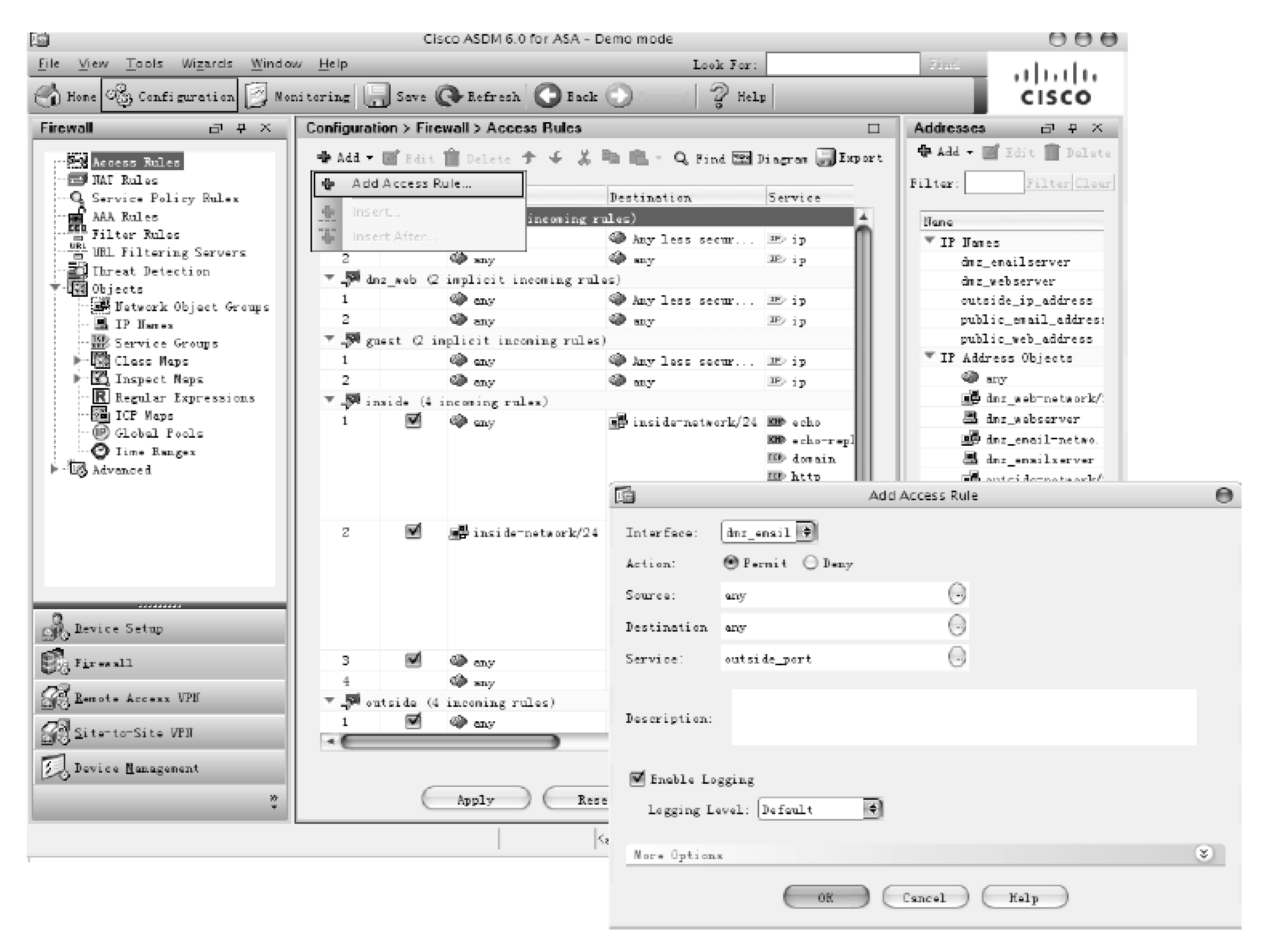


图 8-22　添加访问规则

❸ 选择 Configuration→ Firewall→NAT Rules 结点，并选择 Add NAT Exempt Rule 命令，可以配置 inside 端到 DMZ dns/mail 的访问规则，如图 8-23 所示。

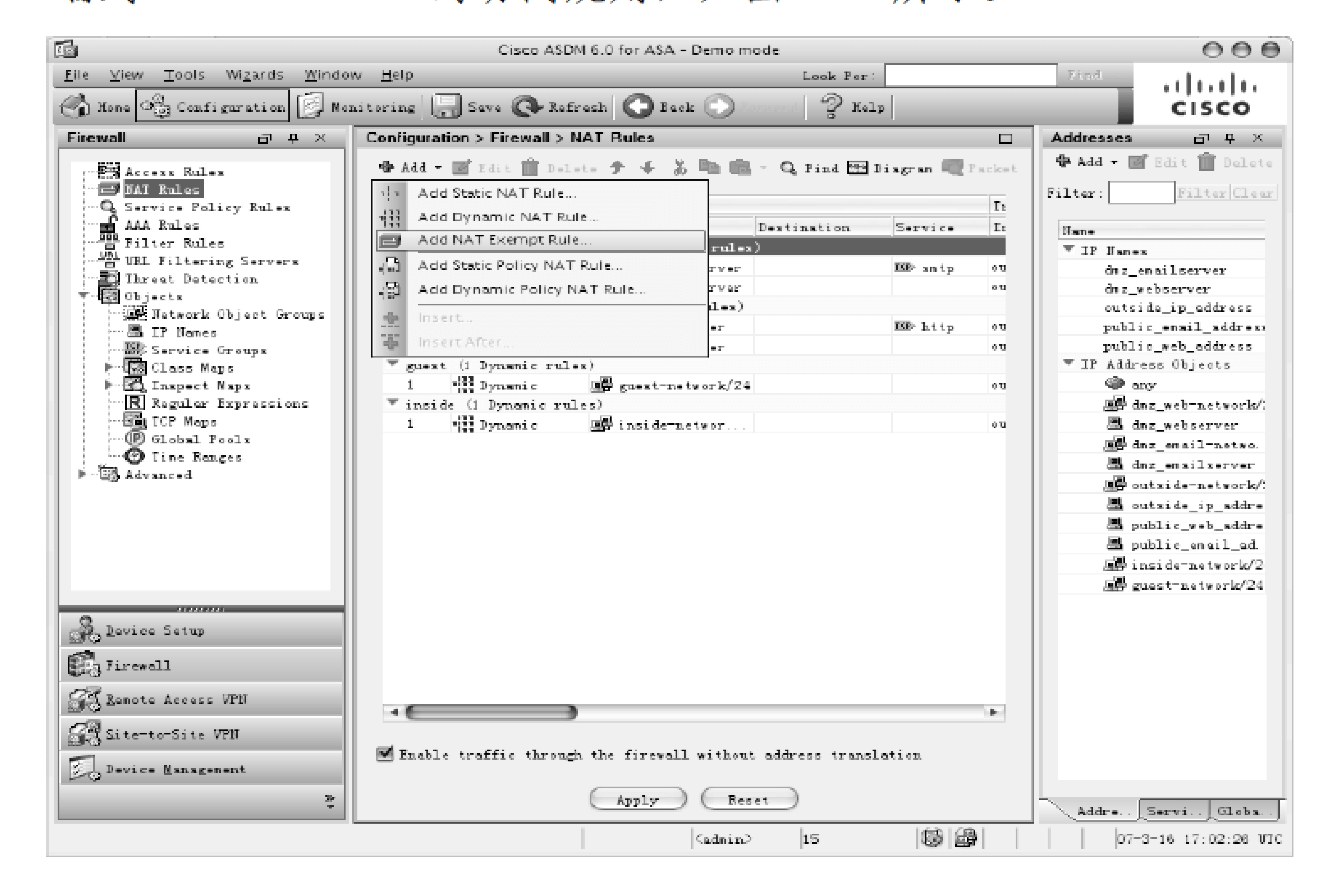


图 8-23　添加 NAT Exempt 规则

❹ 选择 Configuration→Firewall →NAT Rules 结点，并选择 Add Static NAT Rule 命令，可以配置外部网络能够访问到 Web 服务器，如图 8-24 所示。

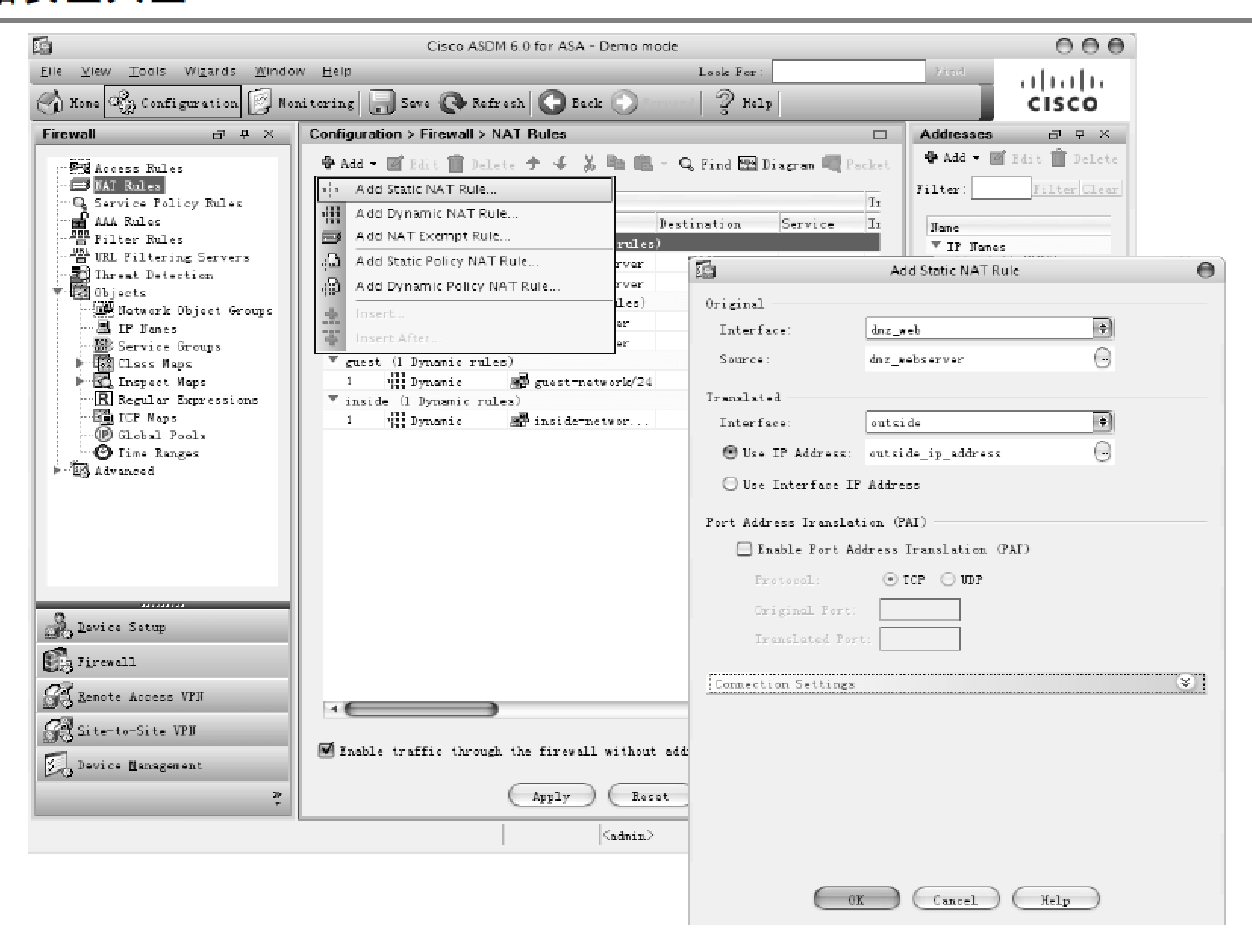


图 8-24　添加外部访问规则

5. 配置应用检测

在 PIX/ASA 防火墙上，可以通过配置应用检测功能，对特定的网络服务进行过滤或流量控制，例如禁止内部员工使用即时通信服务(如 IM)或限制用户 FTP 下载的速率等。

❶ 要控制 IM 软件的使用，可以选择 Configuration→Firewall→ Service Policy Rules 结点，单击 Add 按钮添加相应协议的过滤。在打开的对话框中，选中 IM 复选框，单击 Configure 按钮，如图 8-25 所示。

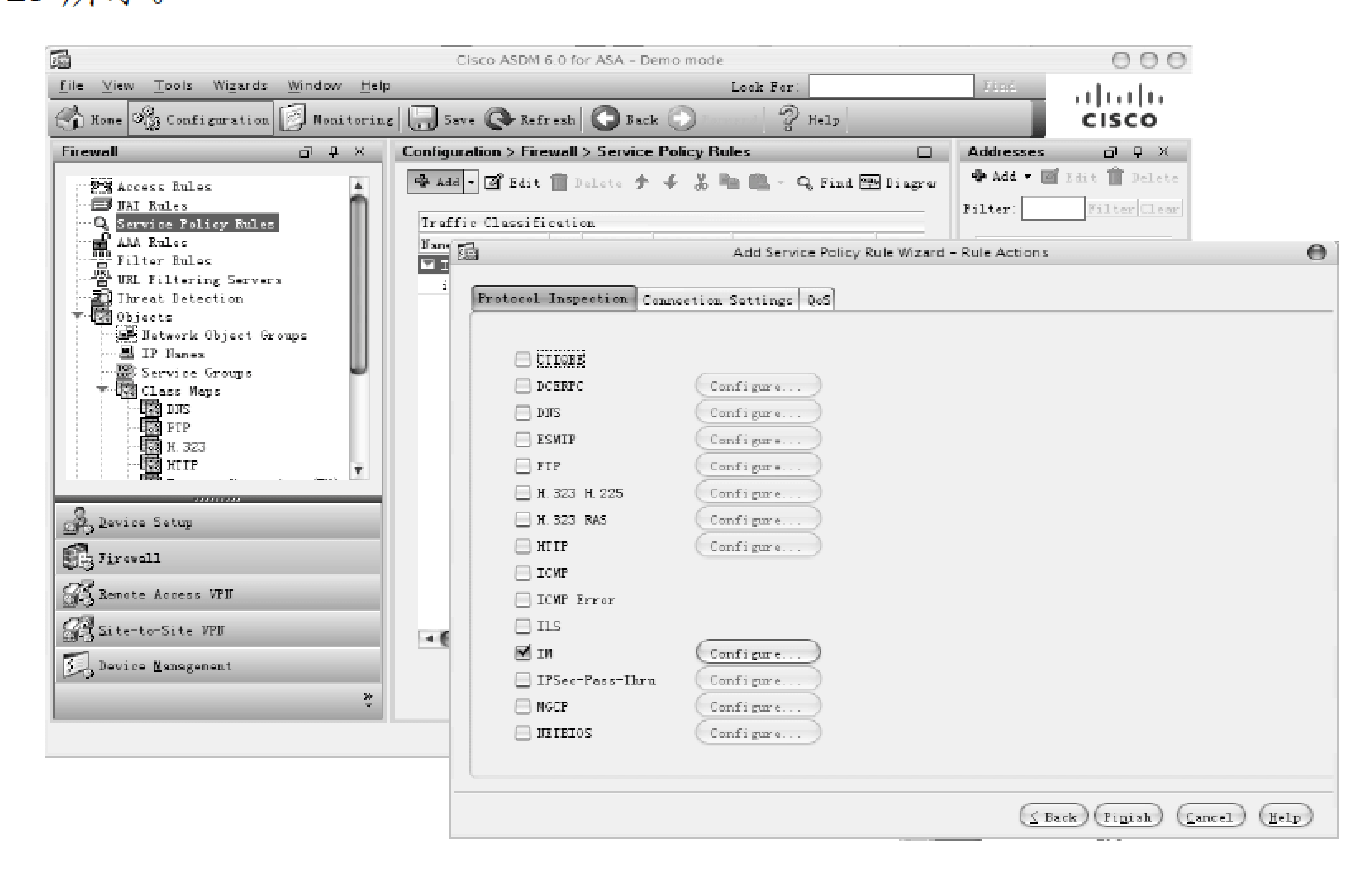


图 8-25　控制 IM 软件的使用

❷ 单击 Add 按钮，添加 IM Inspect Map；在弹出的对话框中，单击 Add 按钮，选择相应的 IM 协议，如图 8-26 所示。

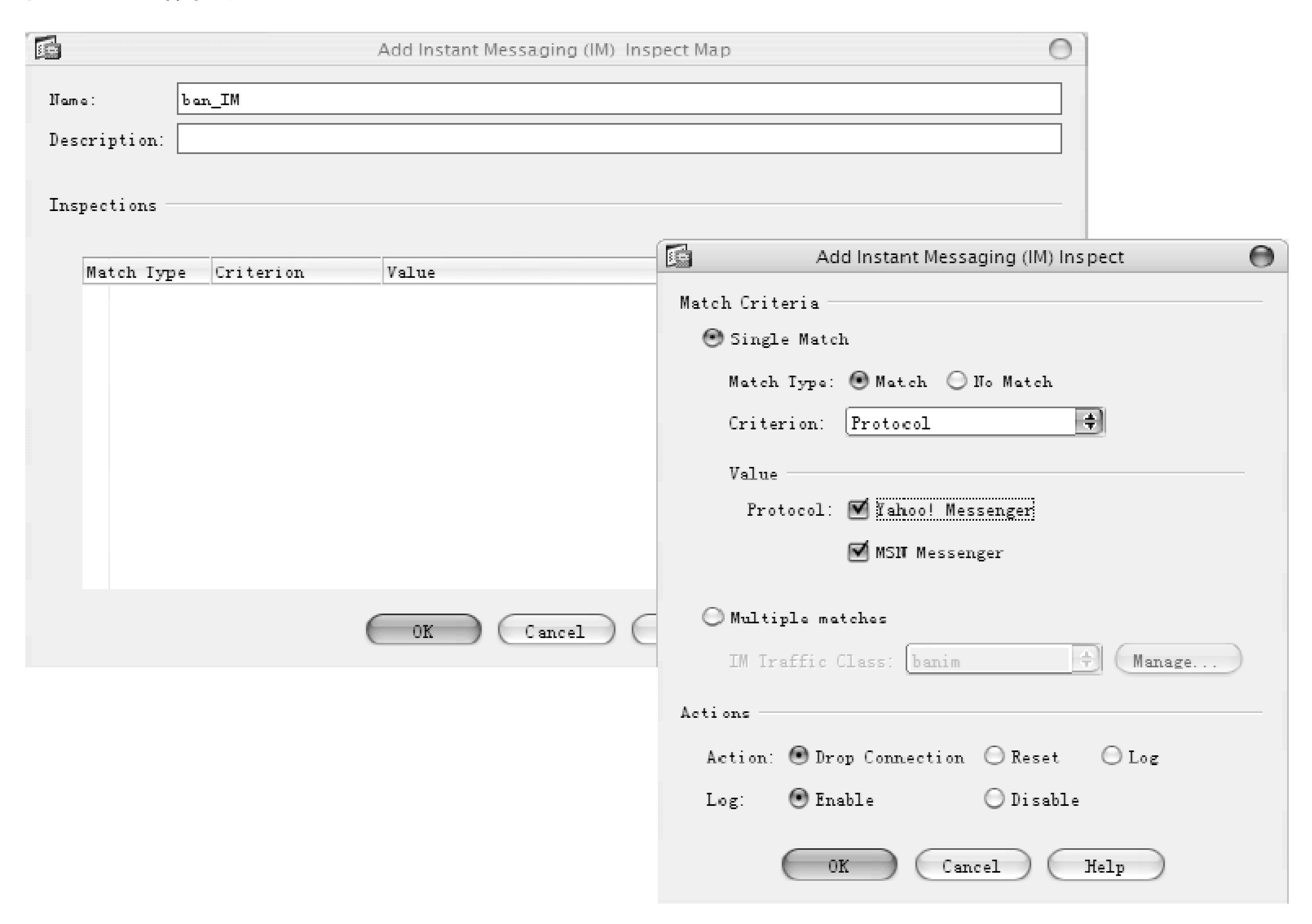


图 8-26　添加 IM 协议

❸ 在 Service Policy Rules 对话框也可以对其他协议进行设置，并控制流量。例如，禁止 FTP 上传命令，并对下载进行速率限制，可以选中 FTP 复选框，单击 Configure 按钮，在弹出的对话框中选中 Use strict FTP 复选框，单击 Add 按钮创建一个 FTP Inspect Map，如图 8-27 所示。

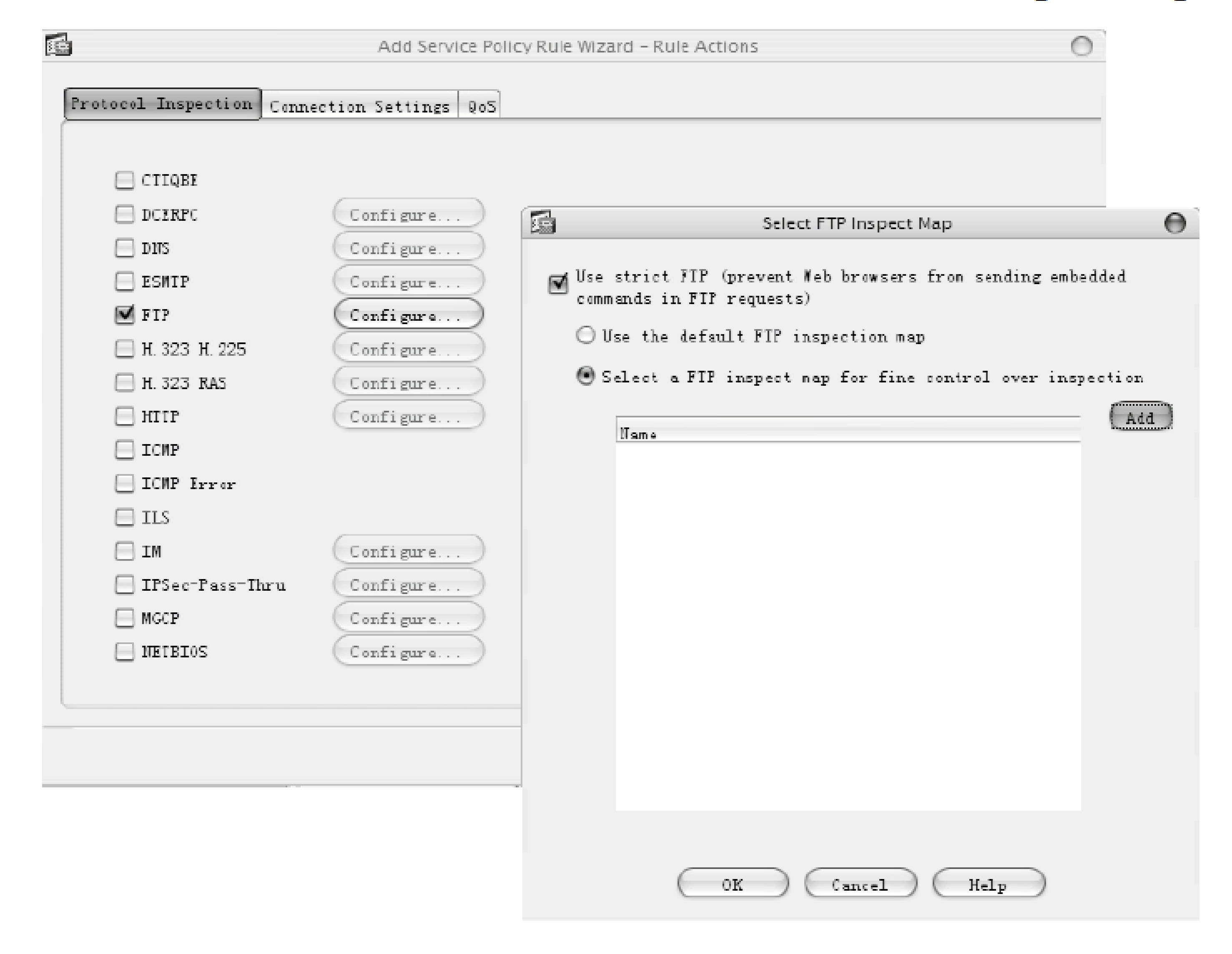


图 8-27　创建 FTP Inspect Map

❹ 在打开的对话框中，单击 Details 按钮，选择 Inspections 选项卡，单击 Add 按钮，在弹出的

对话框中选中 PUT 复选框，禁止上传功能，如图 8-28 所示。单击 OK 按钮。

图 8-28　禁止 FTP 上传功能

❺ 选择 QoS 选项卡，可以配置该应用的 QoS 属性，如图 8-29 所示。

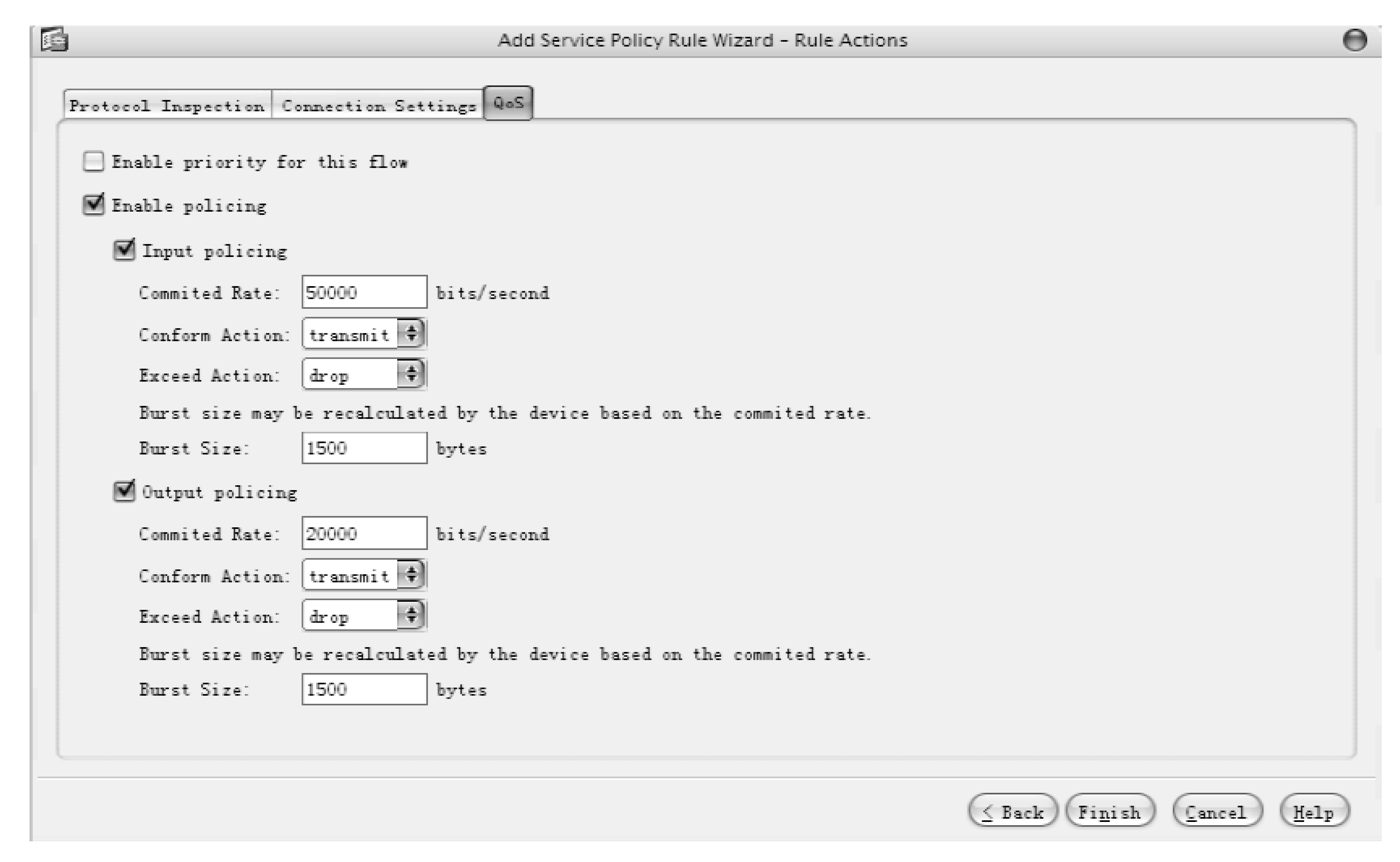


图 8-29　配置禁止 FTP 上传功能的 QoS 属性

❻ 如果要启用 ActiveX 和 Java 过滤功能，可以选择 Configuration→Firewall →Filter Rules 结点，添加 Java、ActiveX 或者 HTTP 过滤规则，如图 8-30 所示。

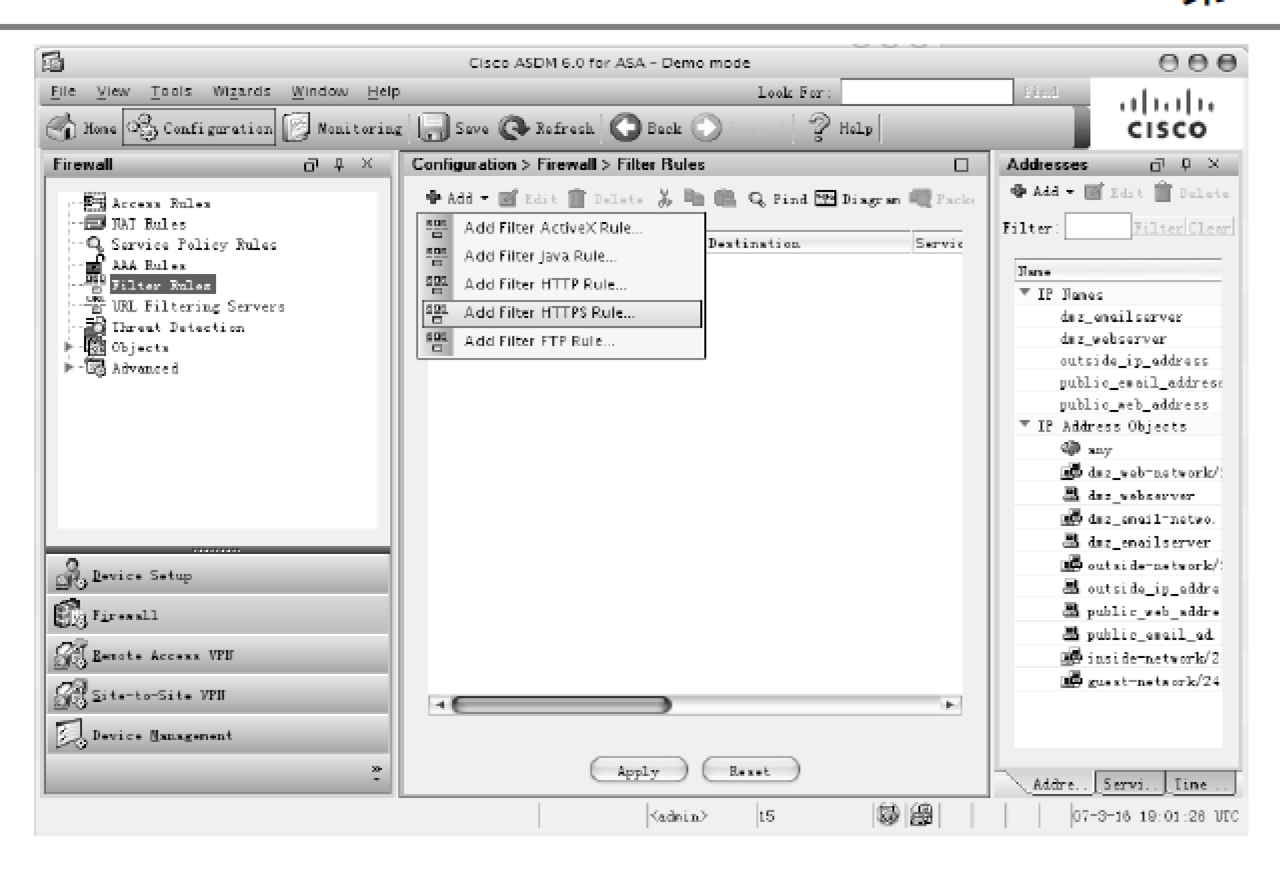


图 8-30　配置 ActiveX 等过滤规则

6. 动态威胁检测

动态威胁检测(Dynamic Threat-Detection)包括如下三个特性。

✧　基本威胁检测(Basic Threat Detection)：对常见攻击进行报警并产生一个报警日志，检测内容包括 DoS 攻击、协议丢包、ACL 禁止流量和其他类型的事件。

✧　扫描威胁检测(Scanning Threat Detection)：对突发的攻击流量进行检测并且实施动态防御，定位攻击源后，通过 Shun 功能对攻击源进行流量屏蔽，并且发送报警日志。

✧　扫描威胁统计(Scanning Threat Statistics)：对现行网络流量进行统计，产生 Host/Port/Protocol 的前 10 名排名日志。

配置动态威胁检测的方法是：选择 Configuration→Firewall →Threat Detection 结点，并在右窗格中选中相应的复选框或单选按钮即可，如图 8-31 所示。

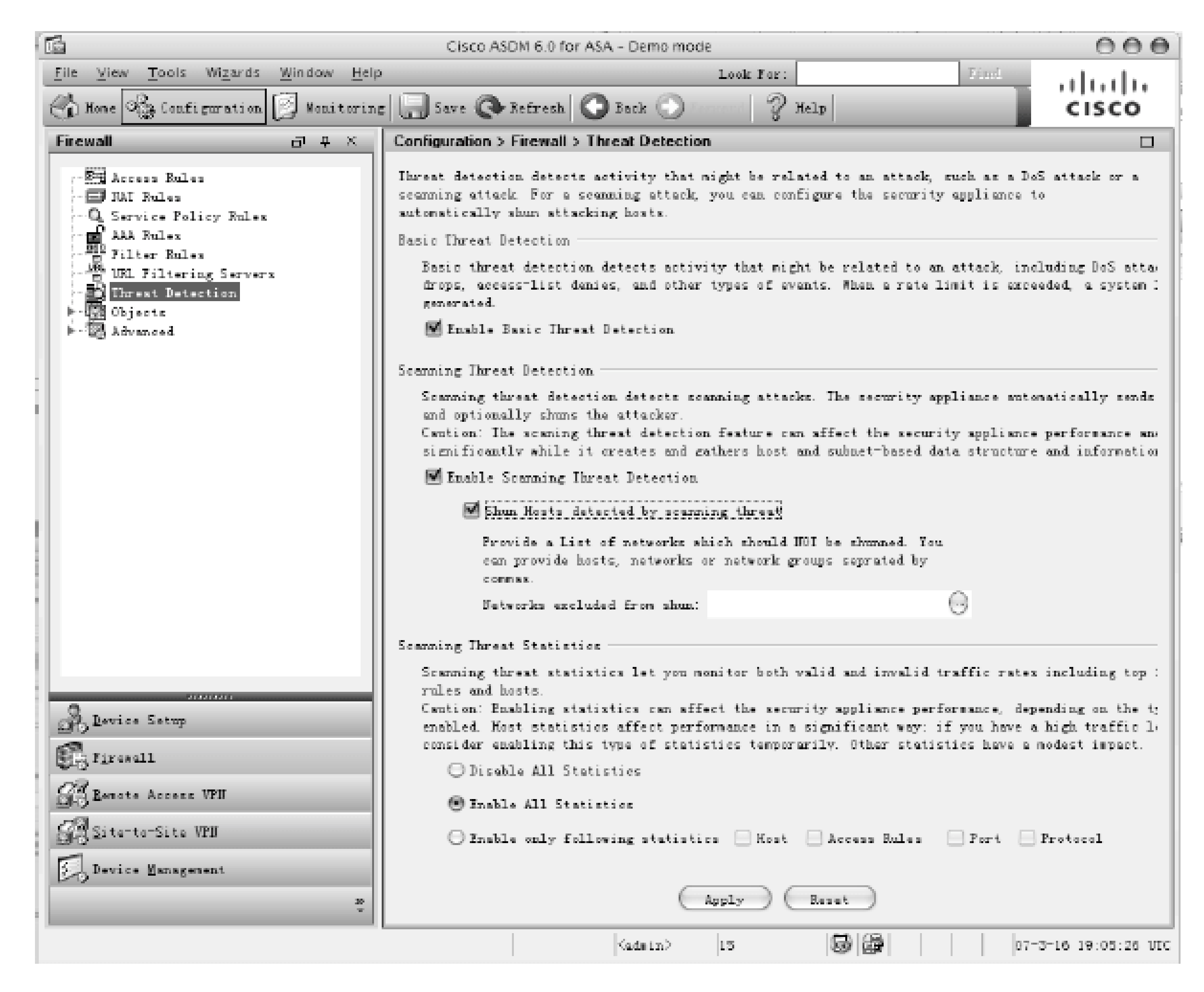


图 8-31　配置动态威胁检测

8.3.3 FWSM 及虚拟防火墙

Cisco 防火墙服务模块(FWSM)可以安装在 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器中，部署在企业外部网的边缘分布层，制定服务器流量策略，提供防火墙功能、入侵检测、虚拟专用网等。FWSM 是一种高速的、集成化的服务模块(如图 8-32 所示)，是性能最高的防火墙解决方案，每个模块的吞吐量能够扩展到 5 Gbps 以上、100 000 CPS，以及 100 万个并发连接。借助多个模块，FWSM 带宽可高达 20 Gbps。

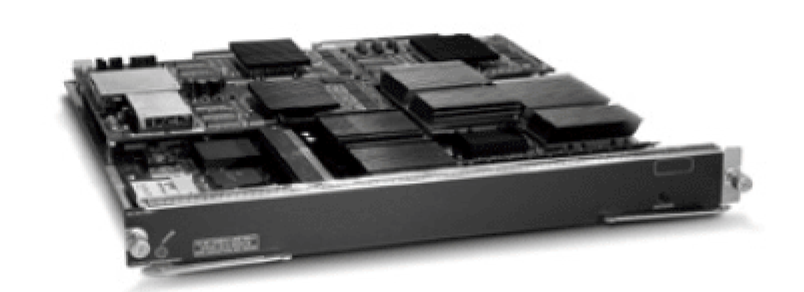


图 8-32　Cisco FWSM 模块

FWSM 采用了 Cisco PIX 技术，并且运行 Cisco PIX 操作系统，可以消除安全漏洞，防止各种可能导致性能降低的损耗。这个系统的核心是一种基于自适应安全算法(ASA)的保护机制，它可以提供面向连接的全状态防火墙功能。利用 ASA，FWSM 可以根据源地址和目的地址，随机的 TCP 序列号、端口号，以及其他 TCP 标志，为一个会话流创建一个连接表条目。FWSM 可以通过对这些连接表条目实施安全策略，控制所有输入和输出的流量。

FWSM 的另一个优点是它集成在核心交换机中，可以对数据中心等业务提供很好的保护，而且不损失性能。FWSM 也和 PIX/ASA 设备一样，可以支持多个虚拟防火墙功能，因此对于分支机构的安全连接，通常可以使用核心交换机上的虚拟防火墙功能实现，并且这种方案节约了成本，也防止了多个防火墙因管理困难而带来的安全隐患。图 8-33 所示为如何部署 FWSM 和虚拟防火墙。

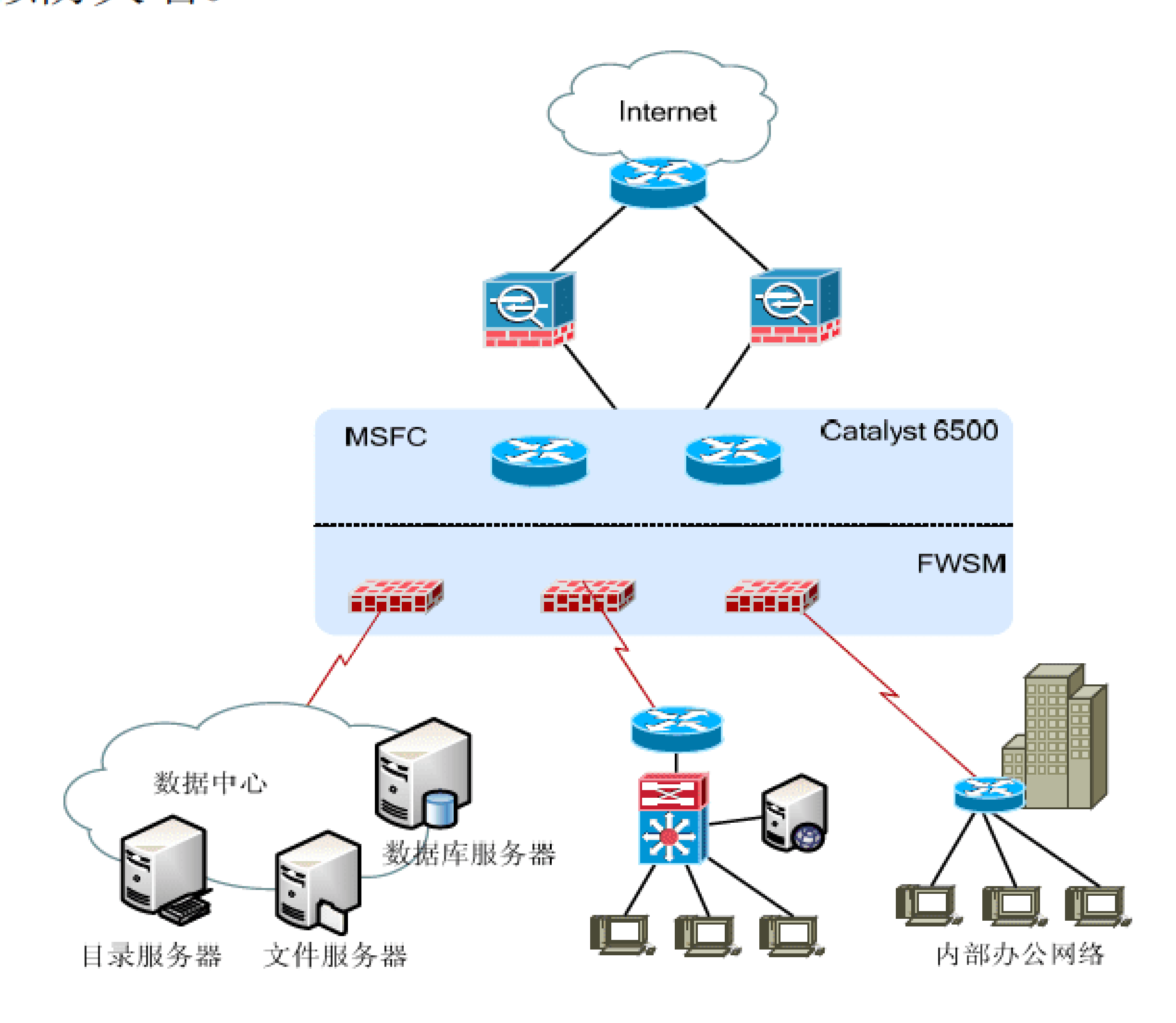


图 8-33　部署 FWSM 和虚拟防火墙

1. 配置 FWSM

由于 FWSM 基于 Cisco PIX，使用大家非常熟悉的 Cisco PIX 管理界面，并保持安全性及网络管理界面，下面简要介绍 FWSM 的配置过程。

❶ 从 Catalyst 6500 登录到 FWSM 模块。

```
SadnessSW#session slot 3 processor 1
The default excape charter is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 … Open

User Access Verification

Password:
Type help or '?' for a list of available commands.
FWSM>enable
Password:*********
FWSM#
```

❷ 输入 Activation-key 序列号，激活 FWSM 模块，然后通过 show version 命令查看 License 信息。

```
FWSM#show version
FWSM Firewall Vesion 3.1(3) <system>
Device Manager version 5.0(1)F

Compiled on Thu 06-Jul-06 12:44 by dalecki
FWSM up 10 mins 43 secs

Hardware:   PIX-525, 1024 MB RAM, CPU Pentium III  1000 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

0: Int: Not Licensed         : irq 5
1: Int: Not Licensed         : irq 7
2: Int: Not Licensed         : irq 11

Licensed features for this platform:
Maximum Interfaces          :1000
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
VPN Peers                  : Unlimited

Serial Number: *********
Running Activation Key: ********************************
Configuration has not been modified since last system restart.
FWSM#
```

❸ 在交换机配置 VLAN，并将相应的接口定义到相应的 VLAN 中。例如，配置的 VLAN 数据库如表 8-1 所示。

表 8-1　VLAN 数据库

Context	Inside	Inside IP	Outside	Outside IP
Admin	Vlan 10	10.74.5.1	Vlan 100	10.74.5.2
A	Vlan 11	10.78.5.1	Vlan 101	10.78.5.2

❹ 将 VLAN 信息添加到 FWSM 中。

```
Cat65(config)#firewall multiple-vlan-interface
Cat65(config)#firewall module 3 vlan-group 1, 2
Cat65(config)#firewall vlan-group 1 10, 11, 100, 101
```

2. 配置虚拟防火墙

FWSM 支持虚拟防火墙的模式，可以同时支持最多 256 个虚拟防火墙。虚拟防火墙可以在一个单一的硬件平台上提供多个防火墙实体。 添加“虚拟”这个形容词是为了表明一个单一的硬件实体可以支持多个防火墙实体。虚拟防火墙的目标是让流经某个虚拟防火墙的用户流量与流经现有防火墙设备的流量不存在明显的区别。换句话说，所有常规的防火墙设备功能及其与外部世界的互动，例如独立管理、独立设置、每个虚拟防火墙专用的系统日志服务器和 AAA 服务器等，以及每个虚拟防火墙的各种内部组件(包括独立路由表、转换数据库、ACL 等)，都将被虚拟化。

下面简要介绍 FWSM 在虚拟防火墙模式的配置方法。

❶ 将 FWSM 工作转换为虚拟防火墙模式。转换后，系统会提醒需要重启系统。

```
SadnessFW(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system Configuration? [confirm]
```

❷ 重新启动系统后，可以通过 show mode 命令查看防火墙当前的工作模式。

```
SadnessFW# show mode
Security context mode: multiple
```

❸ 按照需求创建多个 Context。创建 Context 时必须先创建 Admin Context，然后再创建其他的 Context。

```
FWSM(config)#admin-context admin
FWSM(config)#context admin
FWSM(config-ctx)#allocate-interface vlan10
FWSM(config-ctx)#allocate-interface vlan100
FWSM(config-ctx)#config-url disk:/admin.cfg
FWSM(config-ctx)#context a
FWSM(config-ctx)#allocate-interface vlan11
FWSM(config-ctx)#allocate-interface vlan101
FWSM(config-ctx)#config-url disk:/a.cfg
```

❹ 对于每个 Context，可以将其视为一个虚拟的防火墙，并可以进行独立的控制。

```
FWSM(config)# changeto context admin
FWSM/admin(config)# firewall transparenn
FWSM/admin(config)#int vlan 10
FWSM/admin(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default
FWSM/admin(config)#int vlan 100
FWSM/admin(config-if)#nameif outside
INFO: Security level for "inside" set to 0 by default
```

❺ 对于每个 Context，可以配置打开的 HTTP 服务，用于 ASDM 访问。

```
FWSM(config)# changeto context admin
FWSM/admin(config)# interface BVI 1   //将桥接口作为管理接口
FWSM/admin(config-if)#ip address 192.168.1.1 255.255.255.0
FWSM/admin (config)# http server enable
FWSM/admin (config)# http 192.168.1.0 255.255.255.0 inside
FWSM /admin (config)#enable password Cisco
```

如果是一台 PIX/ASA 则按照如下方式配置 context。

```
SadnessASA(config)#admin-context admin
SadnessASA (config)#context admin
SadnessASA /admin(config-ctx)#allocate-interface m0/0  //将管理接口加入到
Context
SadnessASA /admin(config-ctx)# interface m0/0
SadnessASA /admin(config-if)# ip address 192.168.1.1 255.255.255.0
SadnessASA /admin (config)# http server enable
SadnessASA /admin (config)# http 192.168.1.0 255.255.255.0 inside
SadnessASA /admin (config)#enable password Cisco
```

❻ 在 ASDM 中，也可以对多个 Context 进行管理，如图 8-34 所示。

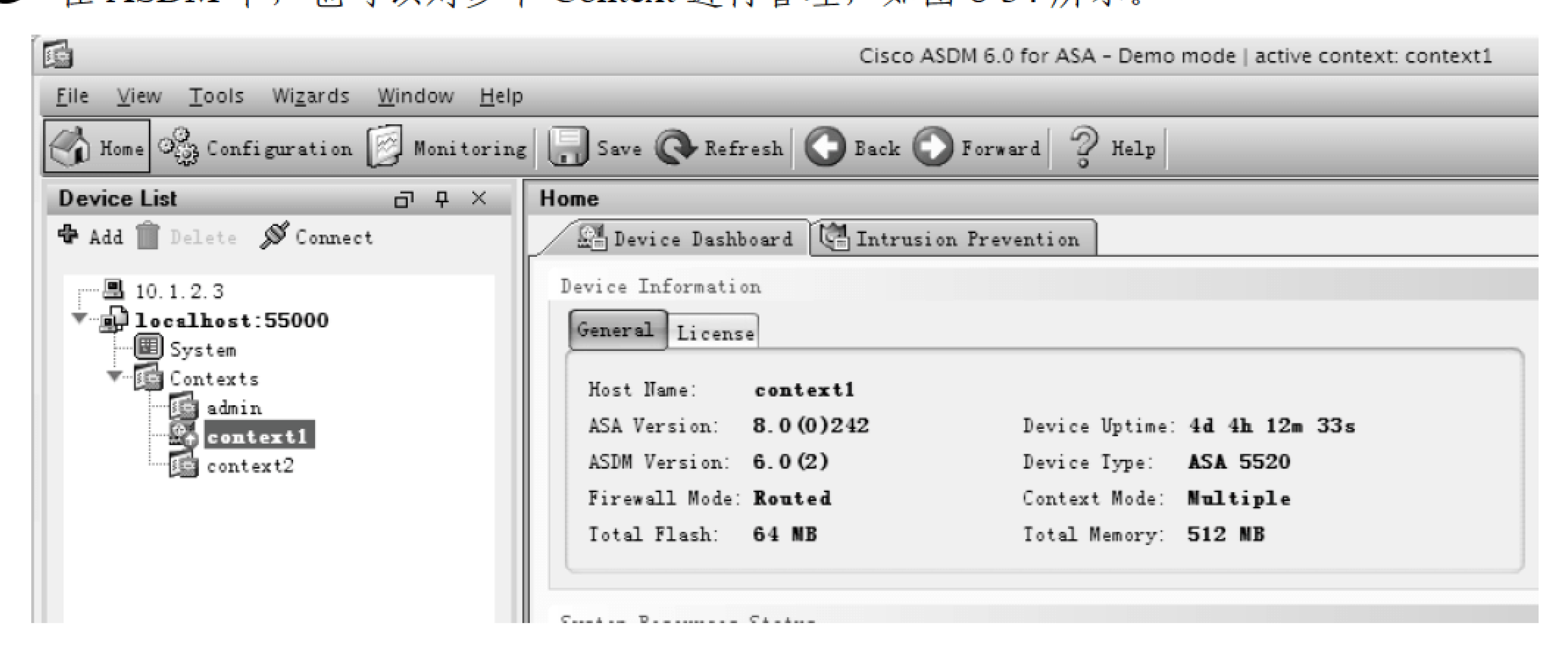


图 8-34　管理多个 Context

❼ 选择 System→Context Management 结点，可以创建或删除 Context，并将不同的接口加入到 Context 中，如图 8-35 所示。

❽ 对于每个 Context，与原有的单模式下的 PIX/ASA/FWSM 一样，可以通过 ASDM 管理，如图 8-36 所示。

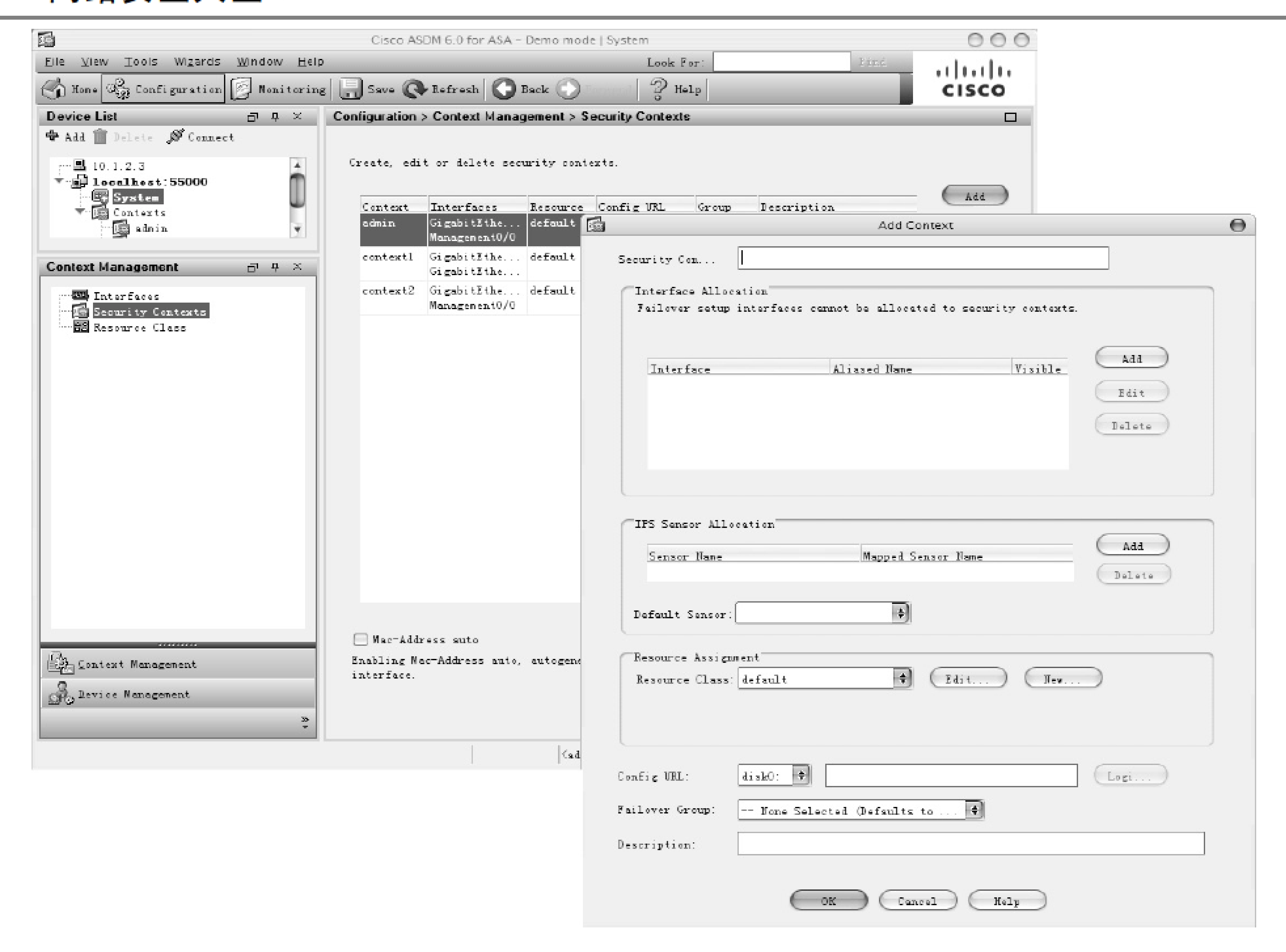


图 8-35　创建 Context

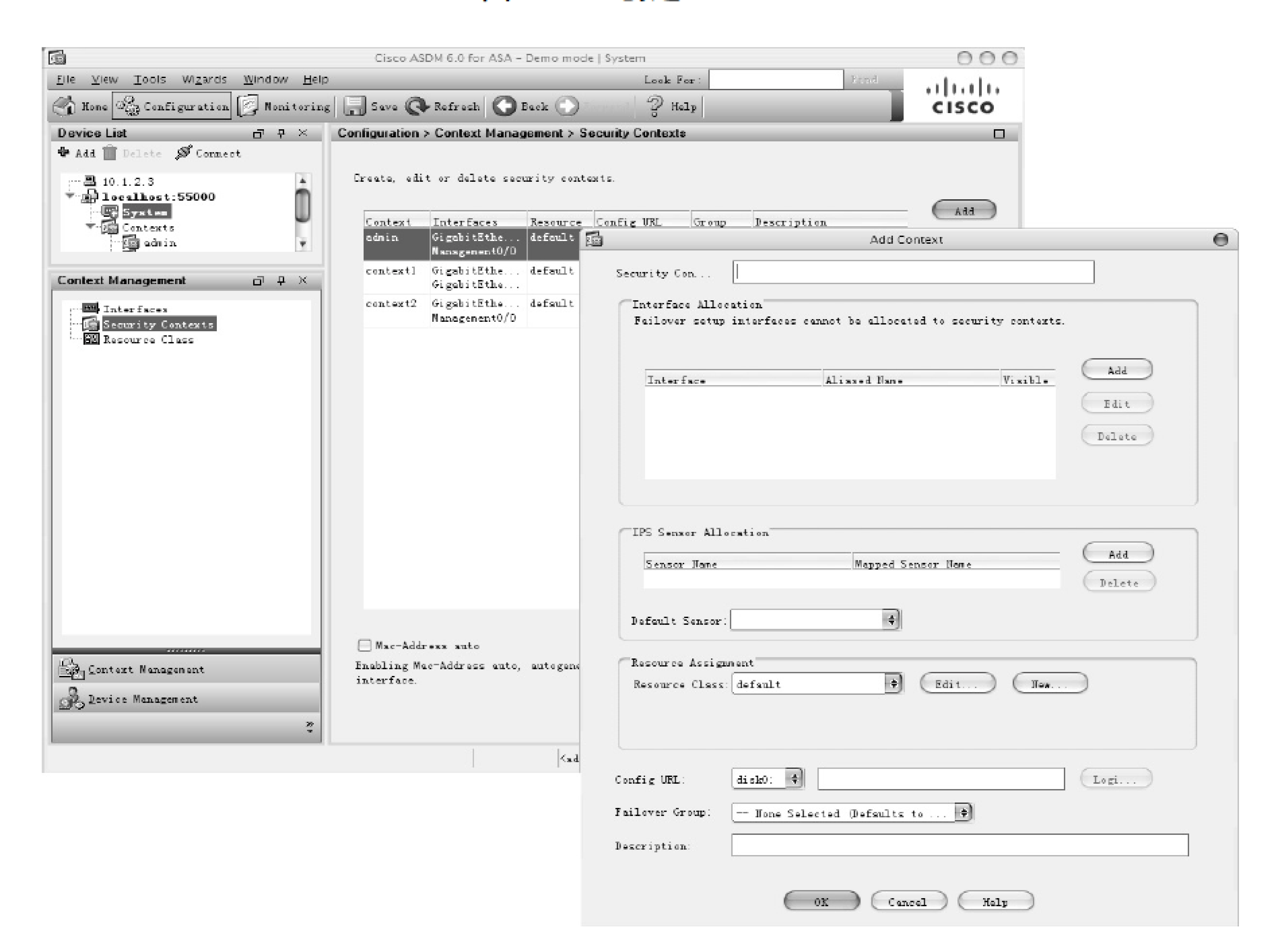


图 8-36　通过 ASDM 管理 Context

❾ 如果防火墙工作在透明模式，还需要为每个 Context 配置静态 NAT，如图 8-37 所示。

图 8-37　为 Context 配置静态 NAT

📖点评与拓展：通过安装 Cisco PIX/ASA 系列防火墙，可以有效地实施防病毒、入侵检测、远程访问等功能，并且 Cisco 提供了基于图像的 ASDM 管理工具，可以方便地监控和配置系统。同时，在 Catalyst 6500 上支持的 FWSM 模块，也提供了一个集中化的防火墙控制管理体系，通过 Context 可以将一台防火墙虚拟成多台设备使用，并且 Cisco ASA 作为 UTM 的代表产品，有效地节约了成本。关于 ASA 的 IPS 和 VPN 功能，将在后续的章节详细介绍。

8.4　微软 ISA 防火墙

应用实例导航：利用 ISA Server 封锁即时通信软件

※场景呈现

Sadness 公司某员工在工作时间通过 QQ、MSN 等 IM 软件将公司的敏感信息传出，公司希望通过有效的方式杜绝员工在工作时间使用这类 IM 软件，但是 ISA Server 2004 主要用于国外，对中国常用的 QQ 等 IM 软件并没有建立相应的访问规则，如图 8-38 所示。同时公司还希望禁止员工在上班时间下载 BT 文件和对某些网站进行访问。



图 8-38　ISA 2004 所支持的 IM 协议

※技术要领

(1)　ISA Server 2004 的安装方法；
(2)　配置 ISA 的访问控制，定义允许、禁止和 URL 过滤的规则；
(3)　向外部网络发布内部服务器，允许外部网络的访问；
(4)　提高访问 Web 服务器的速度，配置 Web 数据的缓冲。

ISA (Internet Security and Acceleration) Server 2004 是高级应用层防火墙、虚拟专用网络 (VPN) 和 Web 缓存的解决方案，它使客户能够通过提高网络安全和性能，轻松地从现有的 IT 投资获得最大收益。ISA Server 2004 有两种可用版本：标准版和企业版。

ISA Server 2004 为各种类型的网络提供了高级保护、易用性以及快速、安全的访问。它尤其适合于保护需要为不同地域设置多重防火墙阵列的大型企业网络，实现运行 Microsoft 客户端和服务器应用程序，例如 Microsoft Office、Microsoft Outlook Web 访问 (OWA)、Microsoft Internet Information Services (IIS)、Office SharePoint Portal Server、路由和远程访问服务、活动目录的目录服务等，以及其他更多的 Microsoft 应用系统、服务器和服务。

ISA Server 2004 包含一个功能完善的应用层感知防火墙，有助于保护各种规模的企业免遭外部和内部威胁的攻击。ISA Server 2004 对 Internet 协议(例如 HTTP)执行深入检查，这使它能检测到许多传统防火墙检测不到的威胁。ISA Server 2004 的集成防火墙和 VPN 体系结构支持对所有 VPN 通信进行有状态过滤和检查。该防火墙还为基于 Microsoft Windows Server 2003 的隔离解决方案提供了 VPN 客户端检查，帮助保护网络免遭通过 VPN 连接进入的攻击。此外，全新的用户界面、向导、模板和一组管理工具可以帮助管理员避免常见的安全配置错误。

8.4.1　安装 ISA Server 2004

与一般软件类似，安装 ISA Server 2004 的方法很简单，其过程如下。

❶ 将 Microsoft ISA Server 2004 安装光盘插入光驱，单击【安装 ISA Server 2004】链接，如

图 8-39 所示。

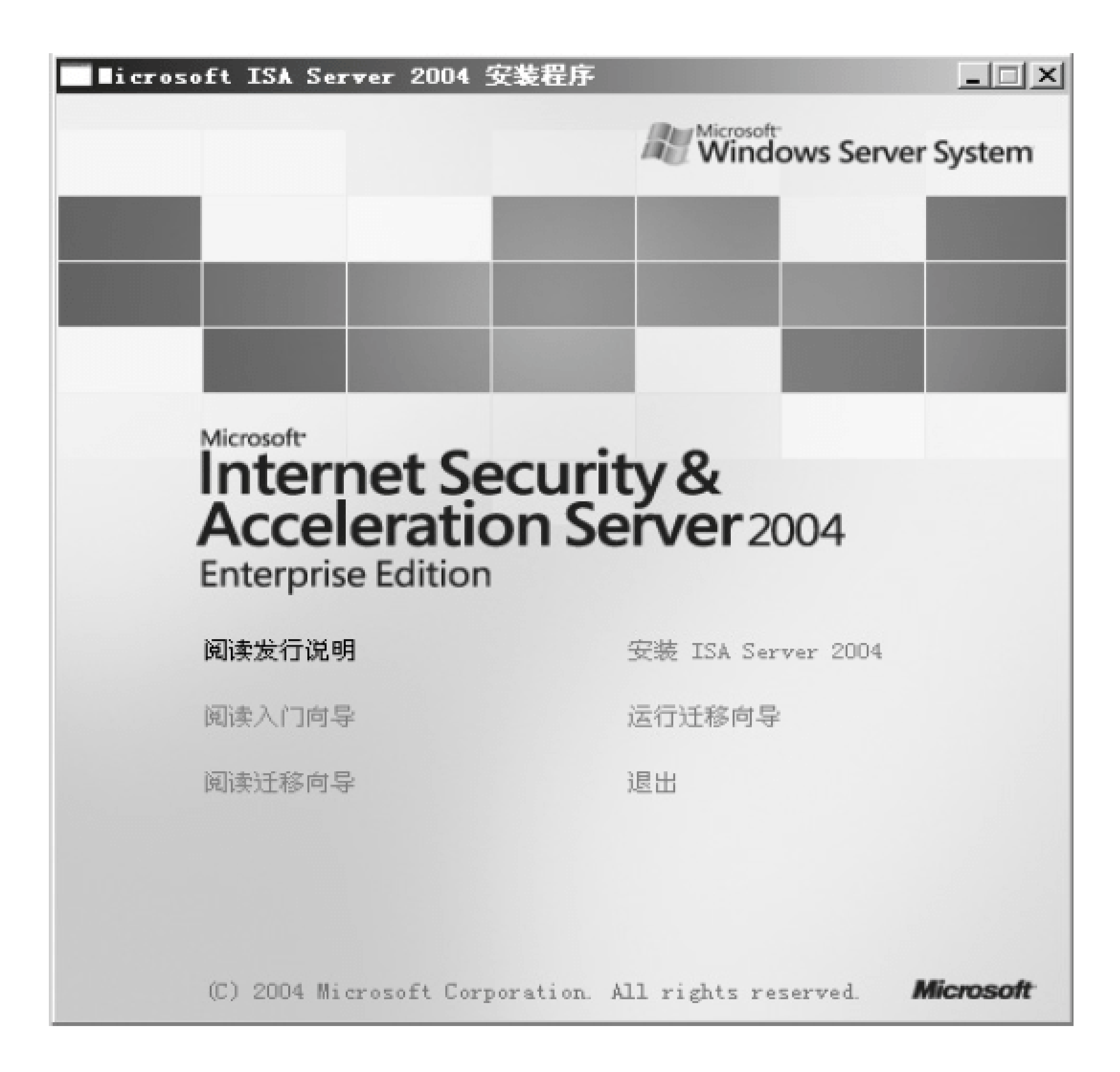


图 8-39　ISA Server 2004 安装界面

❷ 打开 Microsoft ISA Server 2004 安装向导后，接受许可协议并输入安装序列号等信息，单击【下一步】按钮，如图 8-40 所示。

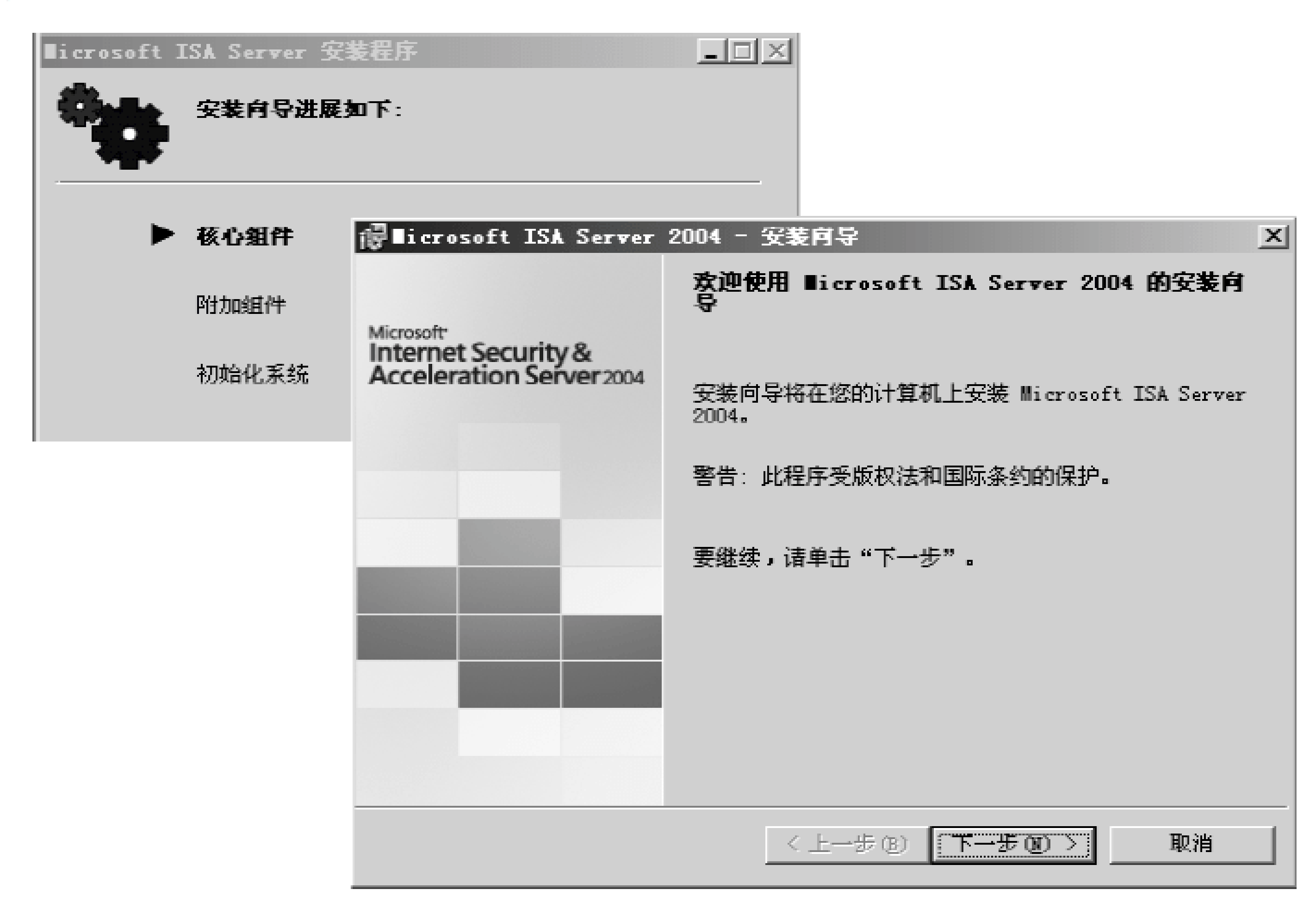


图 8-40　安装 ISA Server 2004

❸ 根据 ISA 服务器的部署方式选择安装方案，如图 8-41 所示。

❹ 选择内部网络地址范围，单击【更改】按钮可以添加内部网络地址范围，完成后单击【下一步】按钮；系统会询问防火墙客户端连接设置，如果局域网中安装了早期的 ISA 防火墙客户端，或者运行 Windows 98/ME/NT，需要选中【允许非加密的防火墙客户端连接】复选框。配置完成后单击【下一步】按钮，如图 8-42 所示。

❺ 系统会提示一些服务将会被重新启动或禁用，单击【下一步】按钮，如图 8-43 所示。

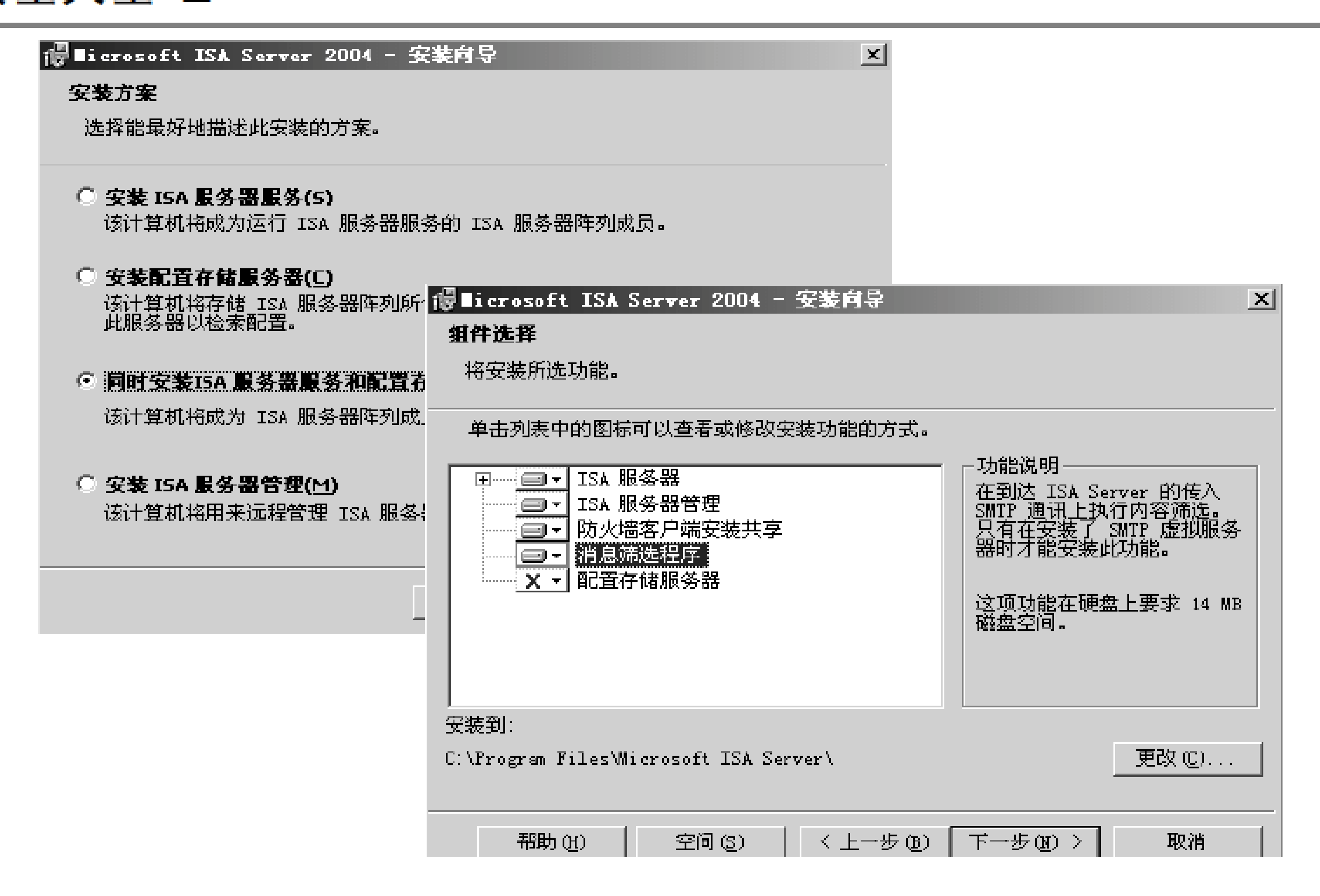


图 8-41　选择 ISA Server 2004 安装方案

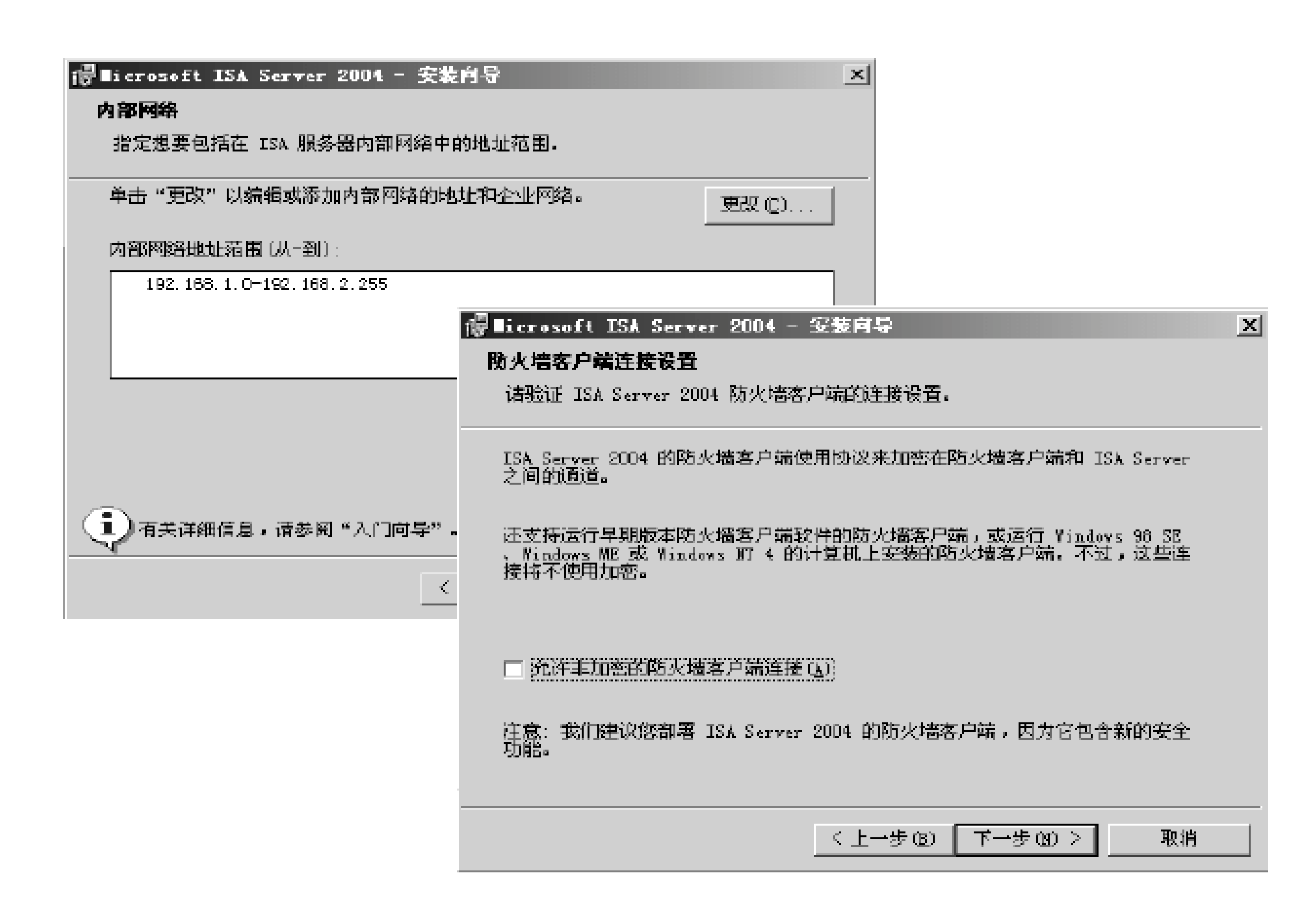


图 8-42　选择防火墙客户端连接设置



图 8-43　安装过程中的服务警告

❻ 安装完成后，将进入 ISA Server 2004 的管理界面，如图 8-44 所示。

图 8-44　ISA Server 2004 管理界面

8.4.2　配置 ISA 访问控制

为了从功能角度描述在被定义的网络间何种通信是被允许的，ISA Server 2004 使用了一组三个规则列表的集合。

✧ 网络规则：此列表定义并描述了网络的拓扑结构。这些规则用于决定两个网络实体间是否具有路由关系，以及何种路由关系被定义(路由还是 NAT)。当网络实体间没有配置任何关系，ISA Server 将丢弃两个网络间的所有通信数据。正确定义网络对象和它们之间的路由关系对于 ISA 2004 显得尤为重要。

✧ 系统策略规则：此列表包含了 30 条 ISA Server 2004 预定义的、应用于本地主机的访问策略。因此，它们控制着 ISA Server 本身“从/到”的通信，并启用诸如验证、网络诊断、日志、远程管理等功能。这些规则 只是“允许”规则，可以启用或者禁用这些规则，或者对其中的一些规则的属性进行少量的修改。

✧ 防火墙策略规则：此列表包含了自定义的所有规则。这是一个经过排序的简单列表，包含了两种可能的规则：访问规则和发布规则。在此列表的最后包含了一条预定义的默认规则：Deny 4 ALL(Deny ALL users use ALL protocols from ALL networks to ALL networks)，拒绝所有用户发起的从所有网络到所有网络的所有协议的访问。这个默认规则不能修改或者删除。所以，任何允许或者阻止的通信都由 ISA Server 2004 的一条明确的规则的来完成。

ISA Server 2004 处理规则的过程如下。

(1) ISA Server 检查网络规则以确定两个网络 实体间是否定义了路由关系，如果源网络与目的网络之间定义了路由关系，ISA Server 2004 将进一步处理客户的出站请求，否则拒绝。

(2) ISA Server 2004 按顺序检查系统策略规则和防火墙策略规则。如果某个系统或者防火墙策略规则允许了此请求，ISA Server 2004 将进一步处理出站请求，否则拒绝。

(3) ISA Serve 2004 再次检查网络规则以确定数据包的路由方式是路由还是 NAT，如果是 Web Proxy 客户端请求对象，ISA Server 2004 也检查 Web 链路规则，以确定请求如何被处理。

1. 定义允许规则

对于内部网络的用户，需要访问外部网络的某些服务(例如 Web 和 FTP)，这就需要定义一些允许规则，其配置操作如下。

❶ 完成 ISA Server 2004 安装后，打开 ISA 管理控制台。在该窗口左侧的控制树中，选择 Sadness ISA→【防火墙策略】结点，可以在右侧窗格中看到系统的一些防火墙策略，如图 8-45 所示。



图 8-45 ISA 防火墙策略

❷ 在窗口左侧的控制树中，选择【阵列】→Sandness ISA→【配置】→【网络】结点，可以在右侧窗格中看到 ISA Server 2004 防火墙连接示意图，如图 8-46 所示。

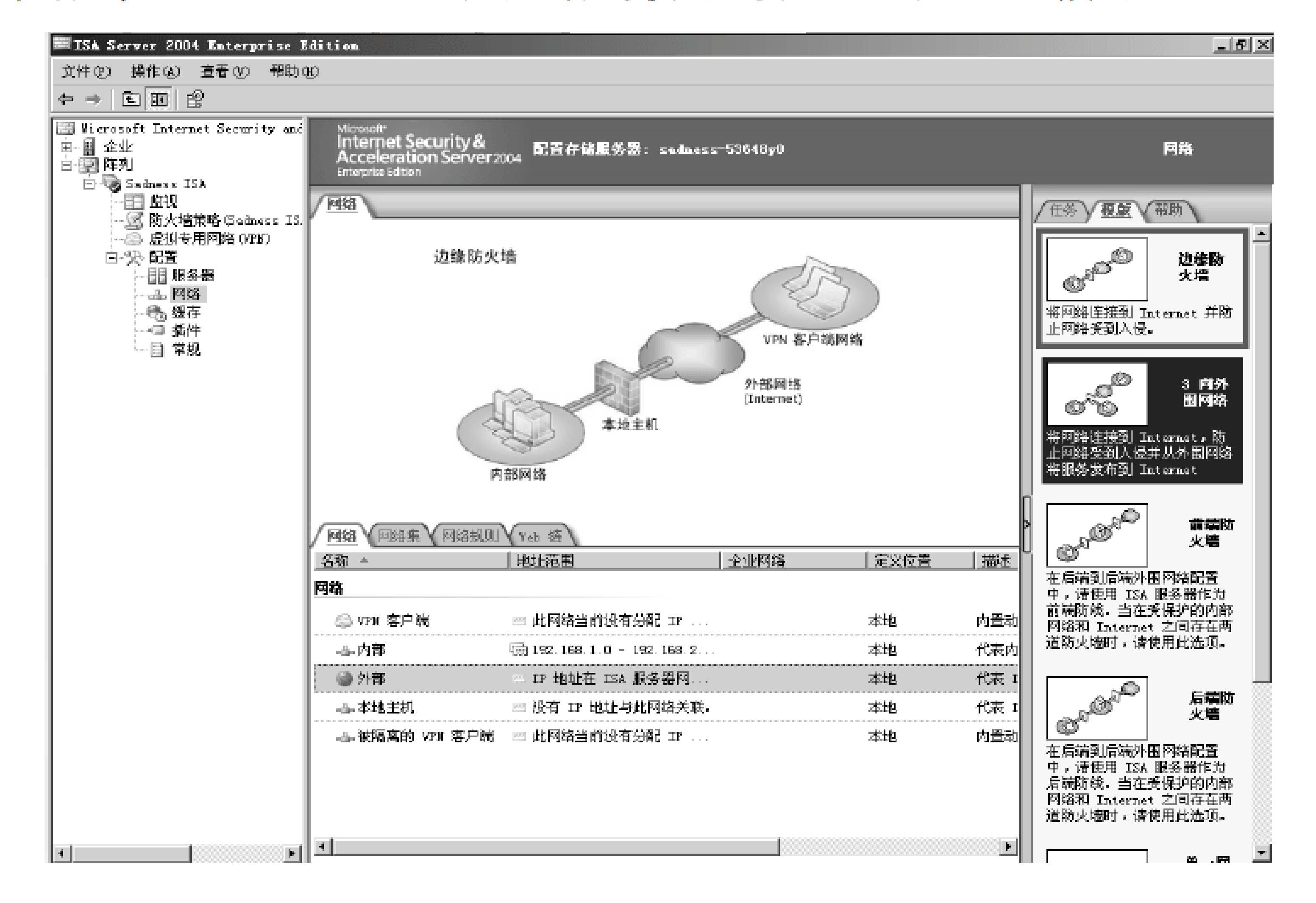


图 8-46 查看防火墙转接示意图

❸ 选择 Sadness ISA→【防火墙策略】结点，右击，在弹出的快捷菜单中选择【新建】→【访问规则】命令，打开新建访问规则向导。输入访问规则的名称，单击【下一步】按钮；在【规则操作】界面中，选中【允许】单选按钮并单击【下一步】按钮，如图 8-47 所示。

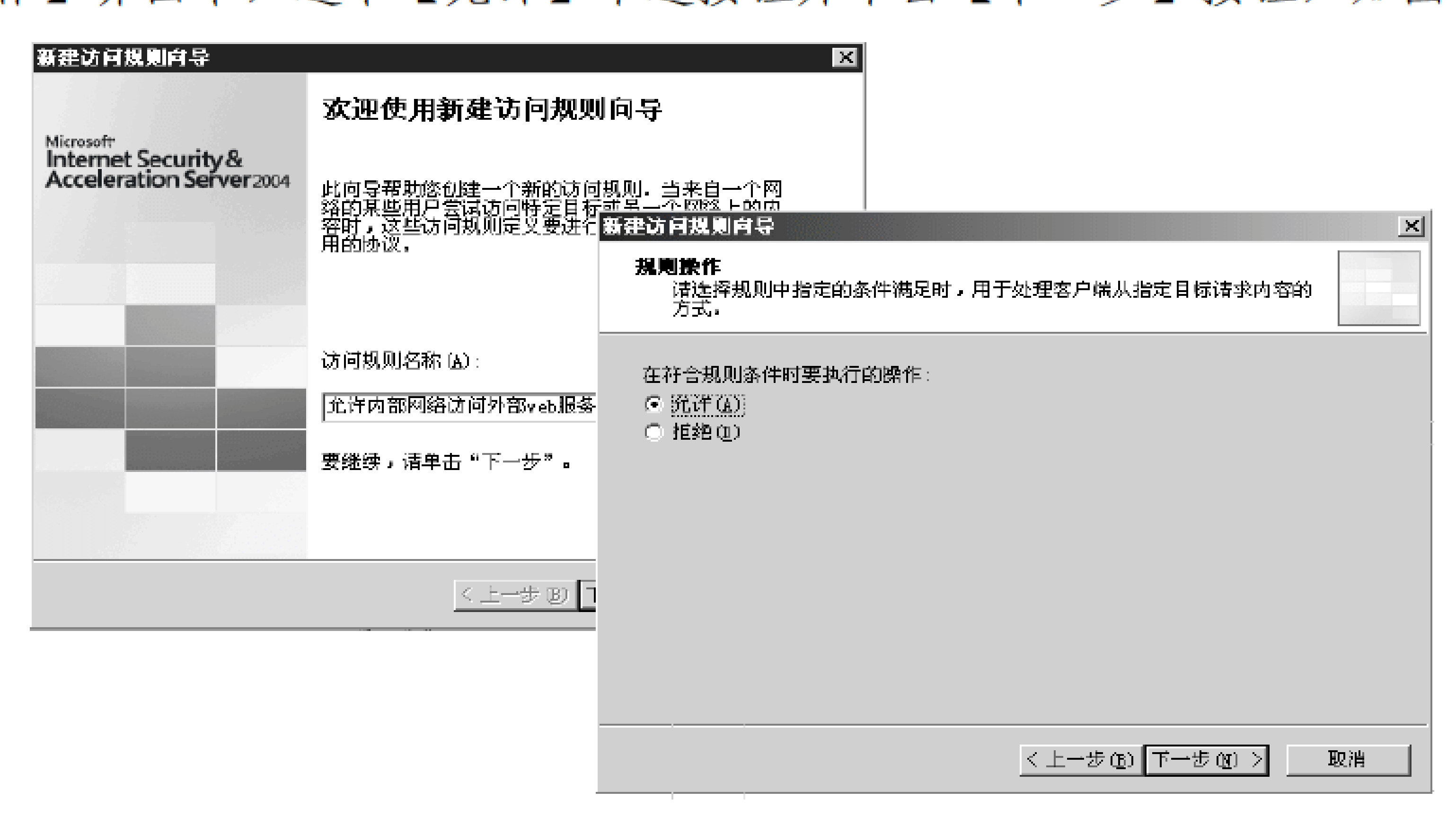


图 8-47　创建访问规则

❹ 在【协议】界面中，选择添加 HTTP、FTP 等此规则应用到的协议，配置完成后，单击【下一步】按钮，如图 8-48 所示。



图 8-48　选择应用规则的协议

❺ 在【访问规则源】界面中，系统将询问信息的指定来源，选择【内部】并单击【下一步】按钮，如图 8-49 所示。

❻ 在【访问规则目标】界面中，系统将询问信息的目的地址，选择【外部】并单击【下一步】按钮，如图 8-50 所示。

❼ 在【用户集】界面页中，选择使用此规则的用户集，仅对具有权限的用户提供访问，确定后单击【下一步】按钮。完成新建访问规则向导后，将显示向导的配置信息，如果配置均正确，单击【完成】按钮，如图 8-51 所示。



图 8-49　选择此规则应用的源网络



图 8-50　选择应用此规则的目标网络

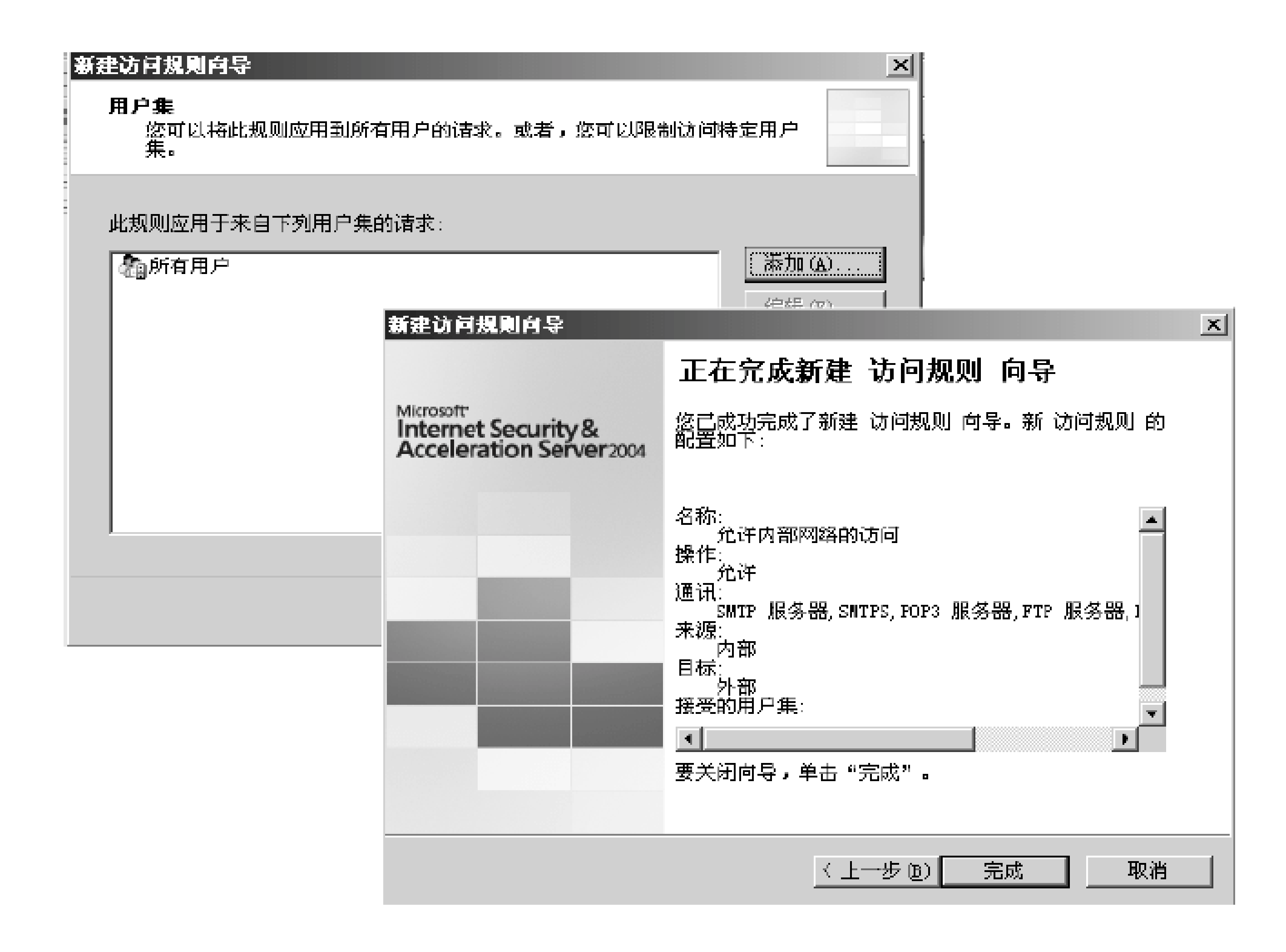


图 8-51　选择用户集

❽ 完成后返回 ISA Server 2004 控制台窗口，单击【应用】按钮即可使规则生效，如图 8-52 所示。



图 8-52 应用新建的访问规则

❾ 对于访问规则，还可以进行详细的定义。选择刚才定义的访问控制条目，右击，在弹出的快捷菜单中选择【属性】命令，在弹出的属性对话框中，定义这条规则的生效时间，如图 8-53 所示。



图 8-53 设置访问规则属性

2. 定义禁止规则

通常访问规则需要包含内网到外网的 HTTP、FTP、Mail、IM 等常规应用，并且管理员还可以定义各种特殊需求。除了允许规则外，公司还可以根据实际情况，禁止某些服务的访问，例如禁止使用 FTP 上传文件、工作时间禁止 P2P 和 IM 等，均可以通过访问控制实现。

在应用实例导航中，Sadness 公司希望禁止员工在工作时间通过 QQ、MSN 等 IM 软件将公司的敏感信息传出。实现这一功能需要定义禁止规则，具体操作步骤如下。

❶ 选择 Sadness ISA→【防火墙策略】结点，右击，在弹出的快捷菜单中选择【新建】→【访问规则】命令，打开新建访问规则向导。

❷ 在弹出的对话框中输入规则名称，单击【下一步】按钮；在【规则操作】界面中，选择【拒绝】单选按钮并单击【下一步】按钮，如图 8-54 所示。

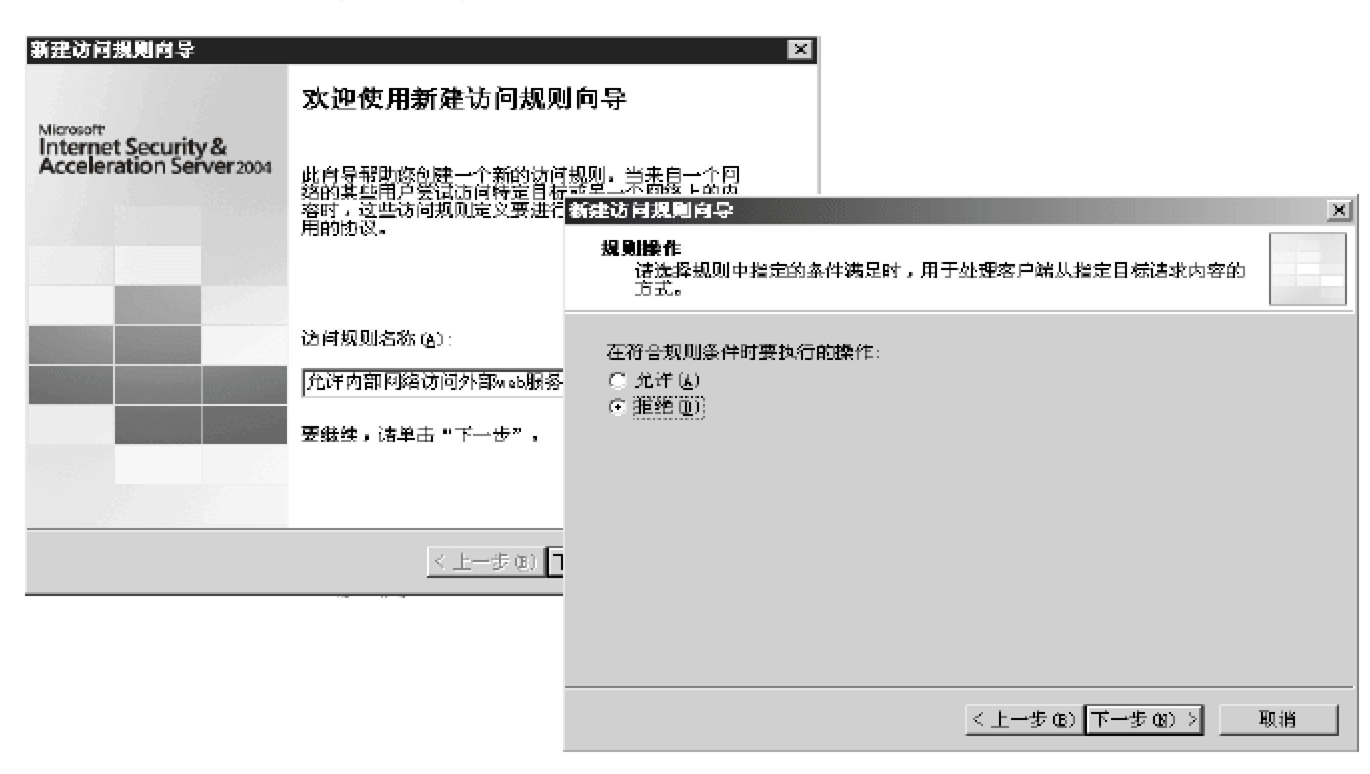


图 8-54　创建访问规则

❸ 在【协议】界面中，单击【添加】按钮，从弹出的对话框中选择相应协议。若【协议】列表框中没有需要的协议(例如 QQ)，可以选择【新建】→【协议】选项来创建一个新协议，如图 8-55 所示。



图 8-55　创建新协议

❹ 在【新建协议定义向导】对话框中，将协议名称定义为 QQ，单击【下一步】按钮，如图 8-56 所示。

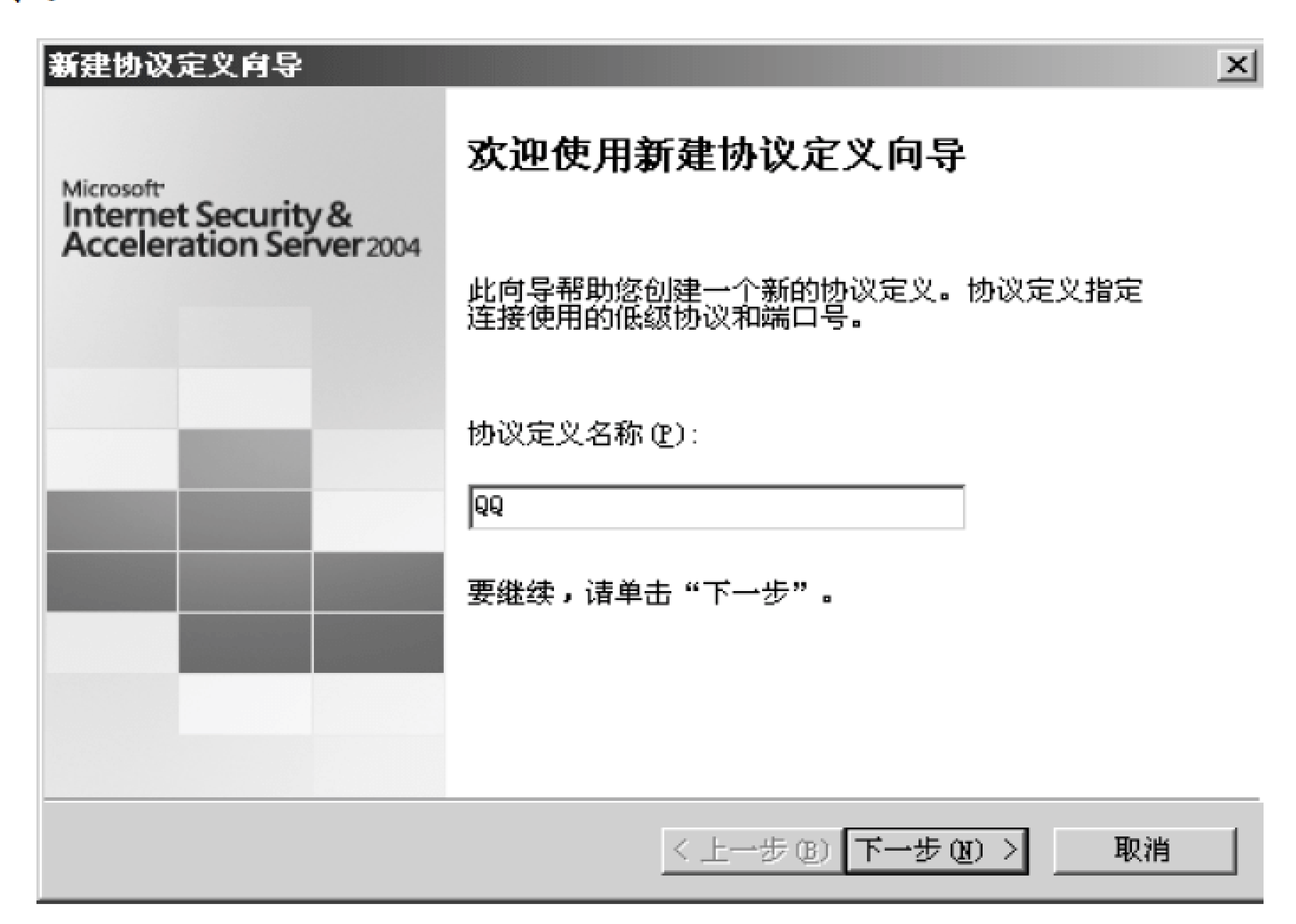


图 8-56 输入协议名称

❺ 在【首要连接信息】界面中，单击【新建】按钮定义端口范围。在【新建/编辑协议连接】对话框中，将【协议类型】下拉列表框设置为 UDP，【端口范围】为从 4000 到 4060，【方向】下拉列表框设置为【发送接收】，如图 8-57 所示，单击【确定】按钮，单击【下一步】按钮。



图 8-57 定义协议使用的端口

❻ 在【辅助连接】界面中，选择不使用辅助连接，如图 8-58 所示。

❼ 返回【协议】界面后，即添加了 QQ 等自定义的协议，如图 8-59 所示。



图 8-58　不使用辅助连接



图 8-59　添加规则应用到的协议

❽ 利用禁止签名来实现 QQ 过滤。在相应的防火墙策略规则上右击，在弹出的快捷菜单中选择【配置 HTTP】命令，如图 8-60 所示。



图 8-60　选择【配置】HTTP 命令

❾ 在弹出的【为规则配置 HTTP 策略】对话框中，选择【签名】选项卡；单击【添加】按钮，在弹出的对话框中设置【名称】下拉列表框为 QQ，【查找范围】下拉列表框为【请求 URL】，【签名】文本框为 tencent.com，如图 8-61 所示。

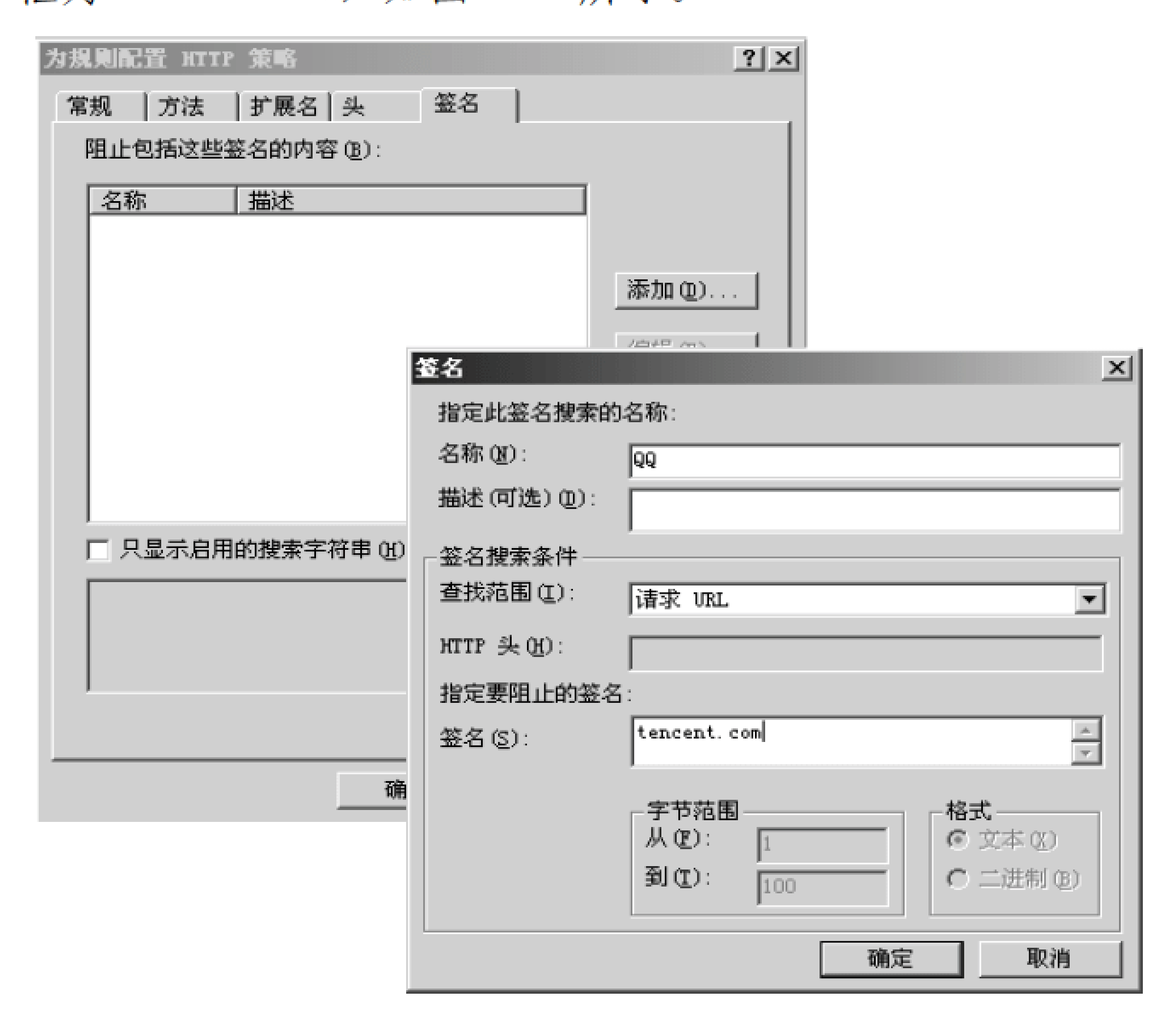


图 8-61　配置 QQ 签名

❿ 对于 MSN 过滤，可以设置【查找范围】为【请求头】，【HTTP 头】为 User-Agent，【签名】为 MSN Messenger；如果是 Windows Messenger，则【签名】为 MSMSGS。

⓫ 对于 BT 过滤，可以设置【查找范围】为【请求头】，【HTTP 头】为【User-Agent 】，【签名】为 BitTorrent，并且在【为规则配置 HTTP 策略】对话框中，选择【扩展名】选项卡，以阻止.torrent 文件，如图 8-62 所示。



图 8-62　阻止 BT 服务

3. 定义 URL 过滤规则

为了保证网络的安全，有时也需要过滤.exe 文件，防止病毒或者蠕虫等文件的执行；同时为了优化网络流量，可以选择禁止.swf、.wmv、.rm 等视频文件。实现上述功能的操作步骤如下。

❶ 选择【防火墙策略】界面右侧的【工具箱】选项卡中的【网络对象】，单击【新建】按钮并选择【URL 集】命令，如图 8-63 所示。



图 8-63 新建 URL 集

❷ 在【新建 URL 集规则元素】对话框中，输入 URL 集的名称，并选择相应的 URL，如图 8-64 所示。

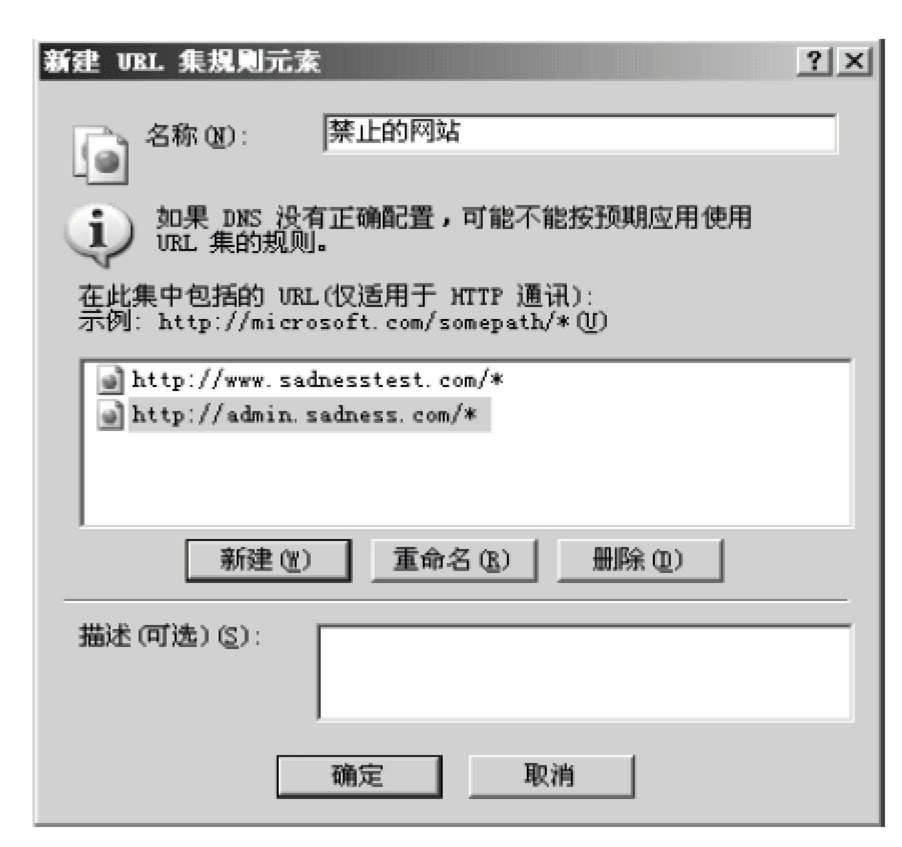
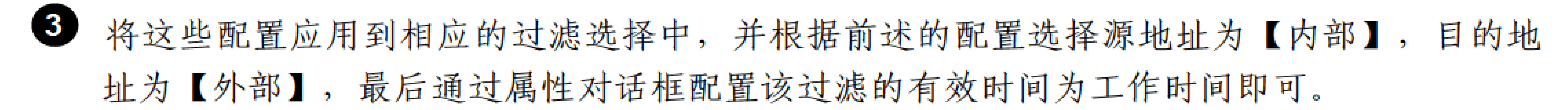


图 8-64 输入协议名称



❸ 将这些配置应用到相应的过滤选择中，并根据前述的配置选择源地址为【内部】，目的地址为【外部】，最后通过属性对话框配置该过滤的有效时间为工作时间即可。

8.4.3　发布服务器

默认情况下，由于 ISA Server 2004 的保护机制，外部网络无法访问内部网络的服务器，因此需要对内网服务器进行发布。下面以发布 Web 服务器为例介绍具体的操作步骤。

❶ 选择 Sadness ISA→【防火墙策略】结点，右击，在弹出的快捷菜单中选择【新建】→【Web 服务器发布规则】命令，如图 8-65 所示，打开新建 Web 发布规则向导。



图 8-65　新建 Web 服务器发布规则

❷ 在新建 Web 发布规则向导欢迎页面中，设置规则的名称，单击【下一步】按钮；在【请选择规则操作】界面中，选中【允许】单选按钮，单击【下一步】按钮，如图 8-66 所示。

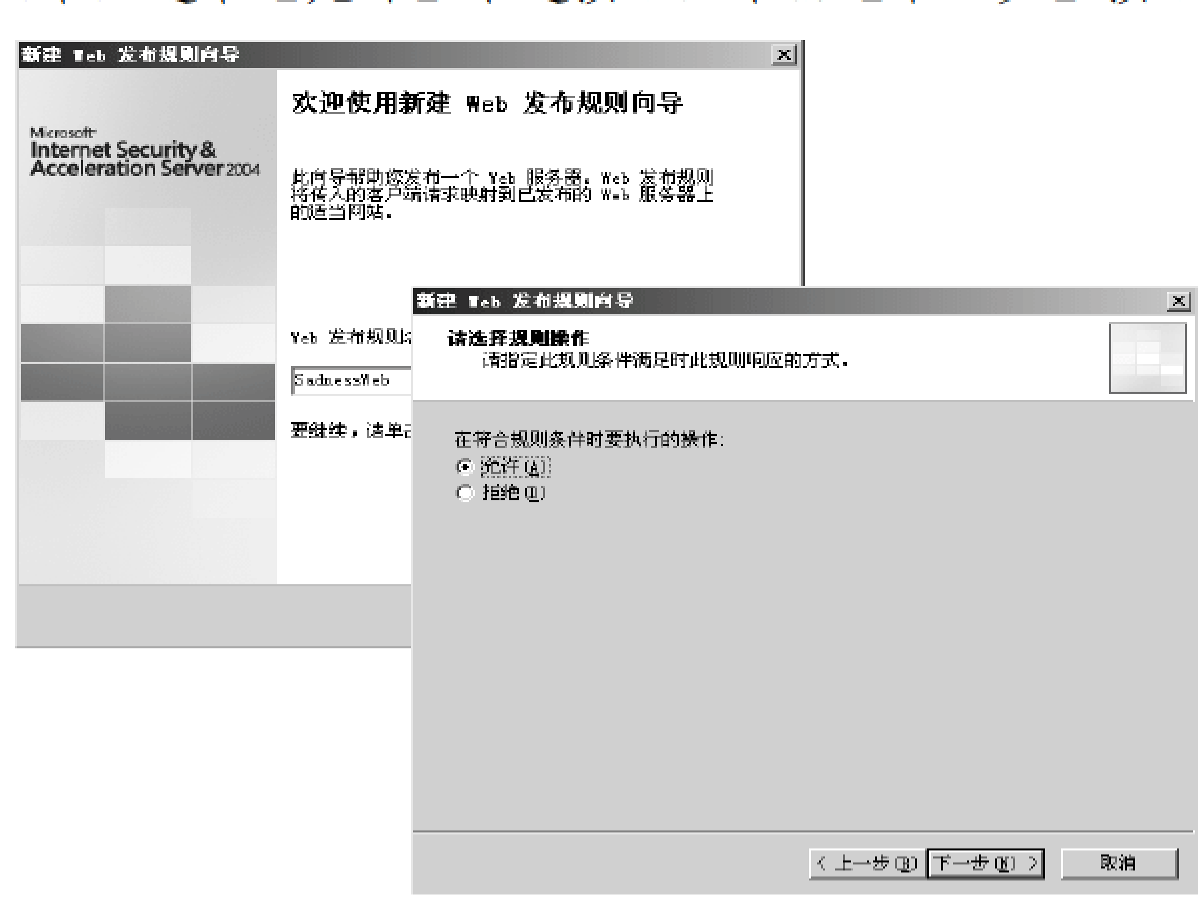


图 8-66　允许发布 Web 服务器

❸ 在【请定义要发布的网站】界面中，在【计算机名称或 IP 地址】文本框中输入 Web 服务器计算机的 IP 地址，将【路径】设置为/*，如图 8-67 所示，单击【下一步】按钮。

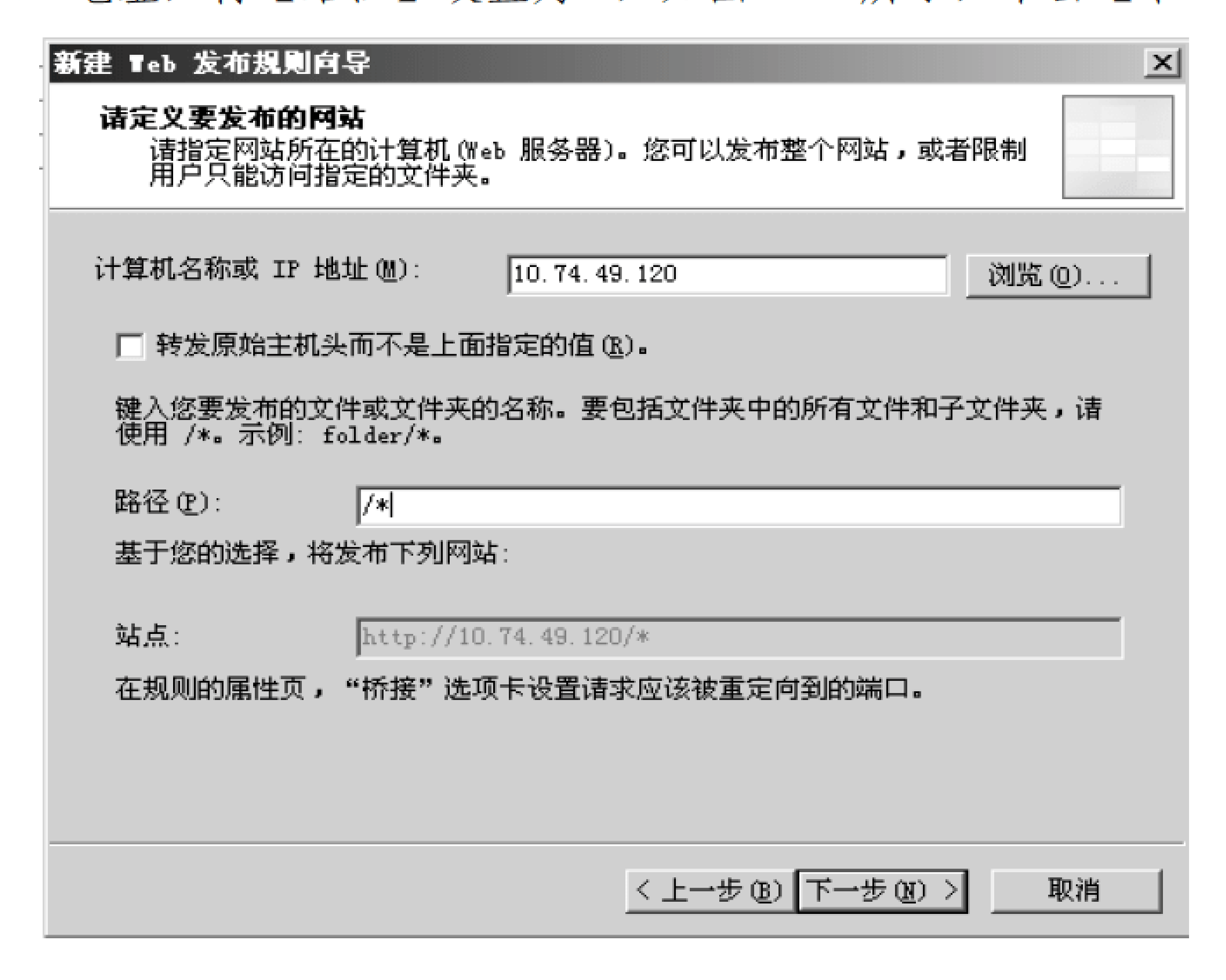


图 8-67　输入 Web 服务器的 IP 地址

❹ 在【公共名称细节】界面中，在【接受请求】下拉列表框中选择【此域名(在以下输入)】，在【公共名称】文本框中输入 Web 站点的主机头名(例如，www.sadness.com)，在【路径(可选)】文本框中输入/*，如图 8-68 所示，单击【下一步】按钮。

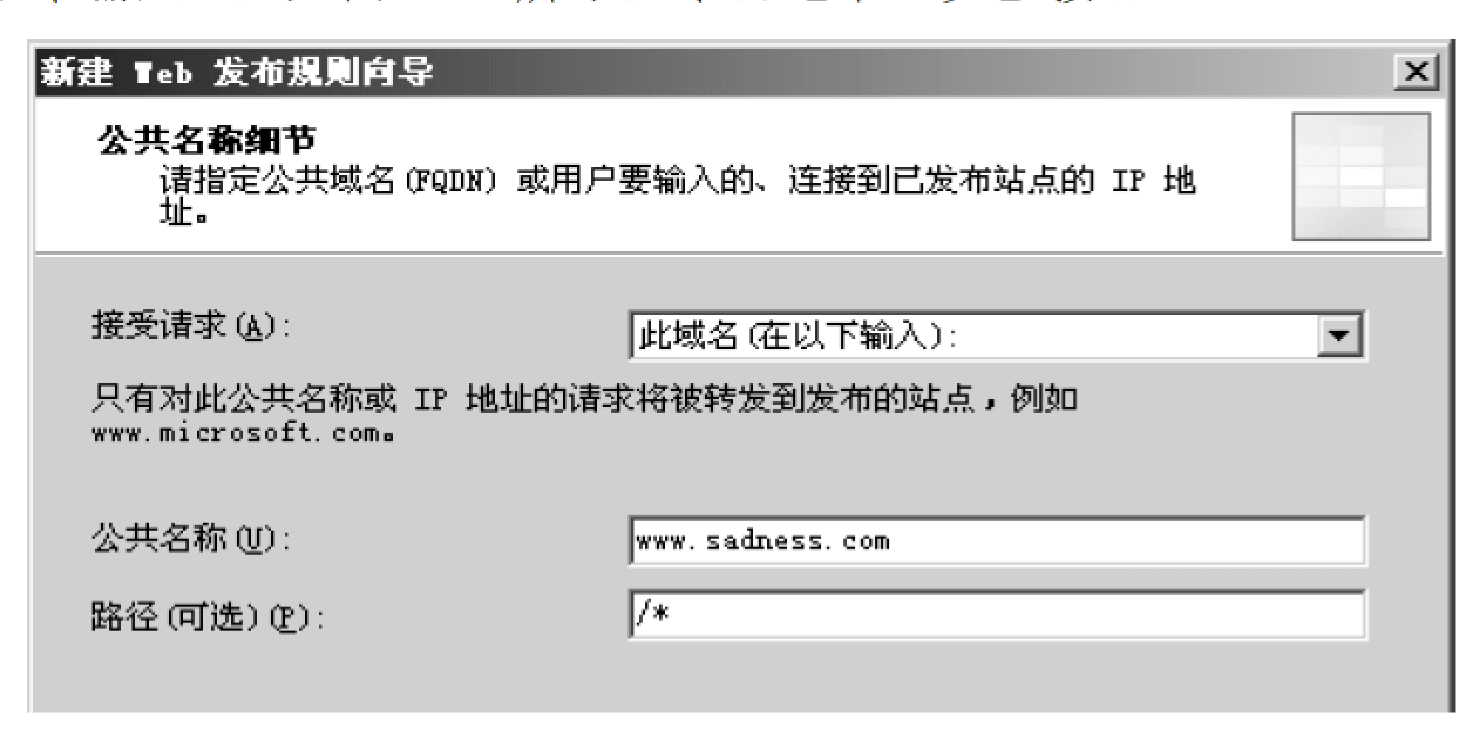


图 8-68　设置 Web 服务器公共域名

❺ 在【选择 Web 侦听器】界面中，选择需要的 Web 侦听器；如果没有，单击【新建】按钮创建一个 Web 侦听器，并输入 Web 侦听器的名称，如图 8-69 所示。

❻ 在【IP 地址】界面中，选择需要监听的 IP 地址为外部网络的所有 IP 地址，单击【下一步】按钮；在【端口指定】界面中，选中【启用 HTTP】复选框，指定端口为 80，如图 8-70 所示。



图 8-69　创建 Web 侦听器



图 8-70　指定监听的 IP 地址和端口

❼ 在【选择 Web 侦听器】界面中，选择刚配置好的 Web 侦听器，单击【下一步】按钮；在【用户集】界面中选择用户集，如图 8-71 所示。



图 8-71 选择 Web 侦听器和用户集

❽ 完成配置后，将 Web 服务器的默认网关设置为 ISA Server 2004 服务器的用于连接到内部网络的 IP 地址即可。

8.4.4 缓冲 Web 数据

ISA 防火墙还可以用来缓冲 Web 数据，从而可提高访问 Web 服务器的速度。其配置方式如下。

❶ 选择【配置】→【缓存】结点，右击，在弹出的快捷菜单中选择【新建】→【缓存规则】命令，如图 8-72 所示。

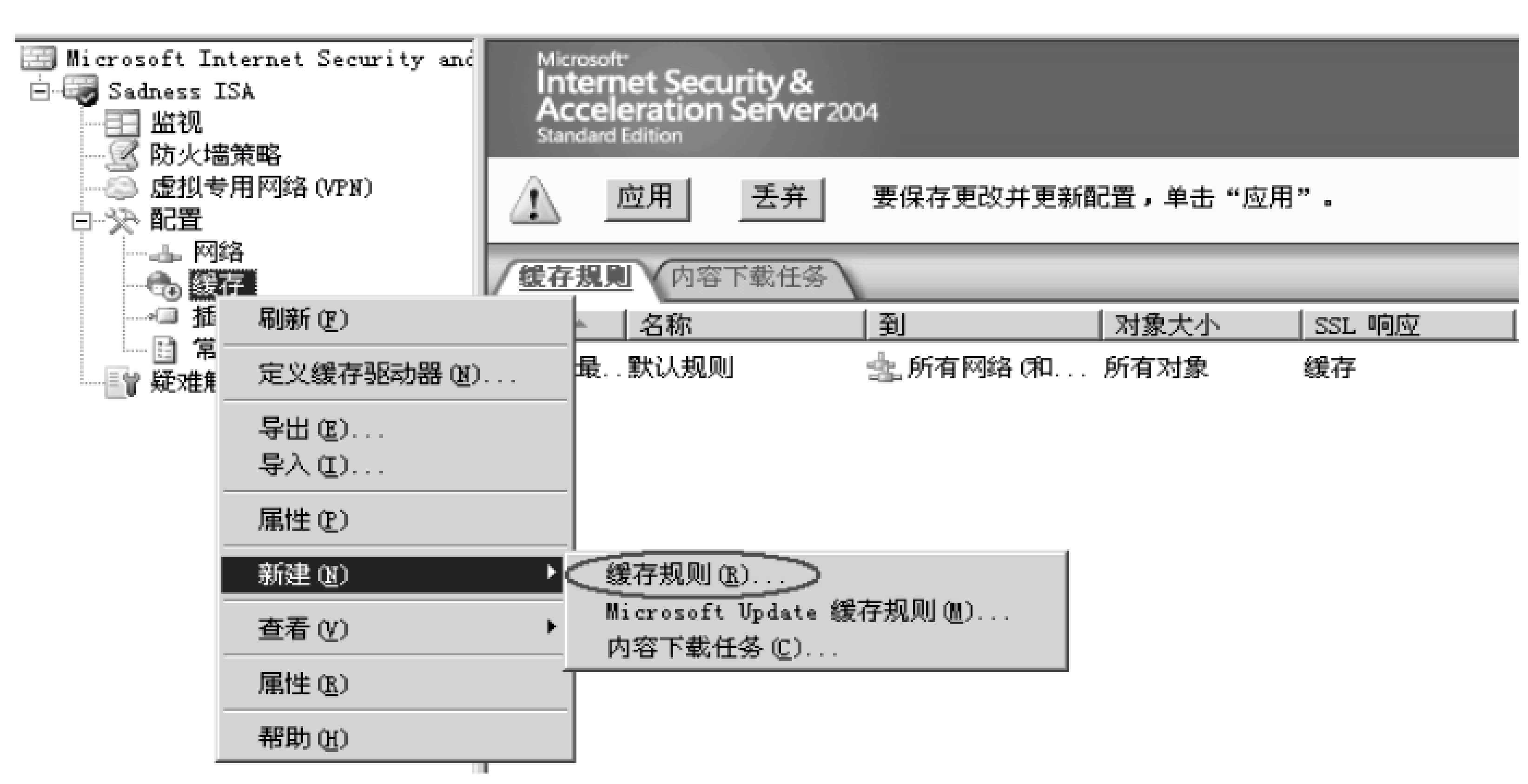


图 8-72 新建缓存规则

❷ 输入规则名，并将缓存规则目标应用的网络实体定义为【外部】，如图 8-73 所示。



图 8-73　设置目标

❸ 在【内容检索】界面中，指定缓存中存储对象被请求时的检索方式。接受默认设置，单击【下一步】按钮，如图 8-74 所示。

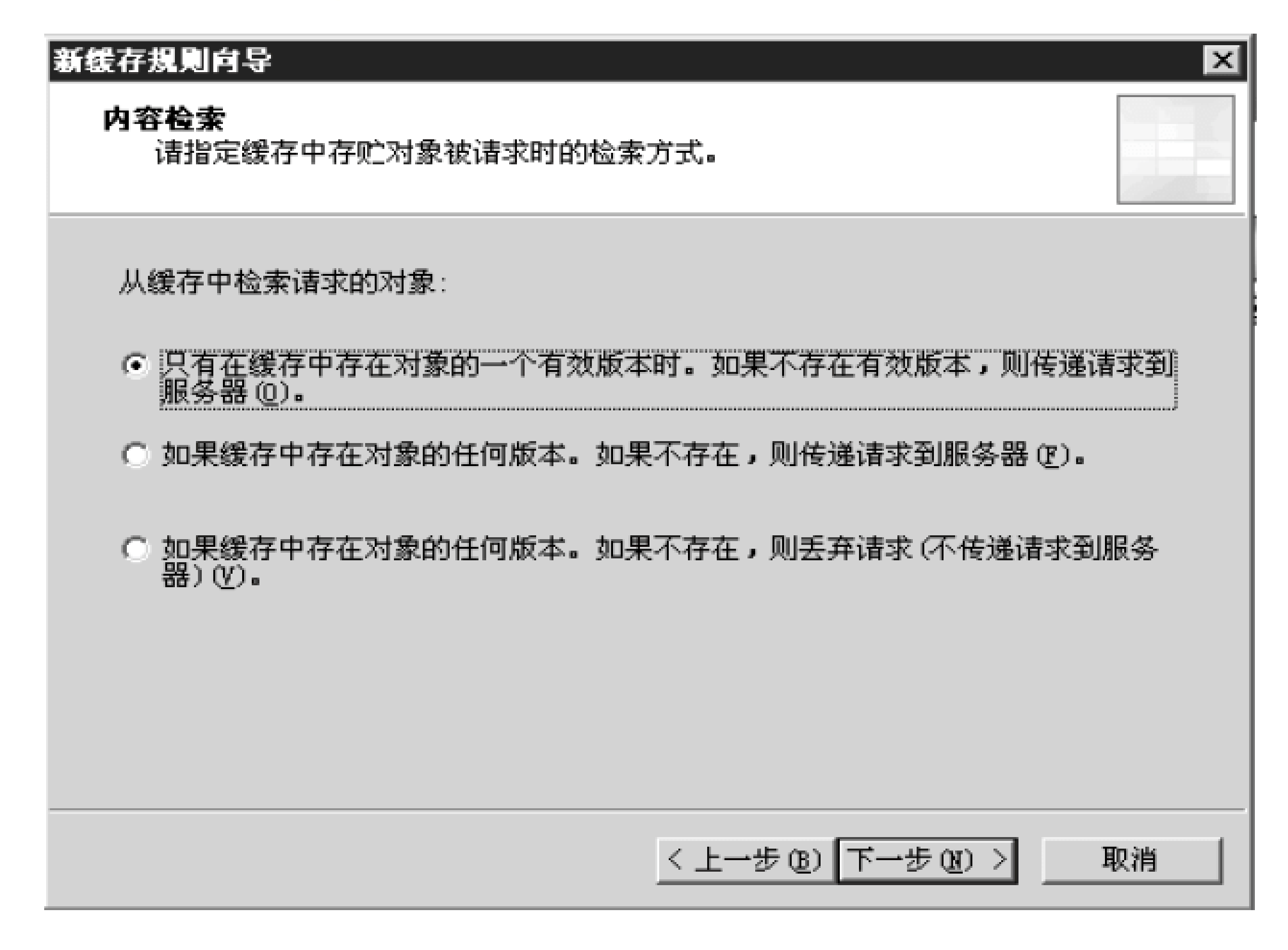


图 8-74　选择检索方式

❹ 在【缓存内容】界面中，指定检索的内容是否存储在缓存中。接受默认设置，单击【下一步】按钮；在【缓存高级配置】界面中，设置最大的缓存对象以及是否缓存 SSL 响应，如图 8-75 所示，设置完毕后单击【下一步】按钮。



图 8-75　选择缓存内容和缓存高级配置

❺ 在【HTTP 缓存】界面中，指定是否启用 HTTP 缓存，单击【下一步】按钮；在【FTP 缓存】界面中，指定是否启用 FTP 缓存，如图 8-76 所示，设置完毕后单击【下一步】按钮。

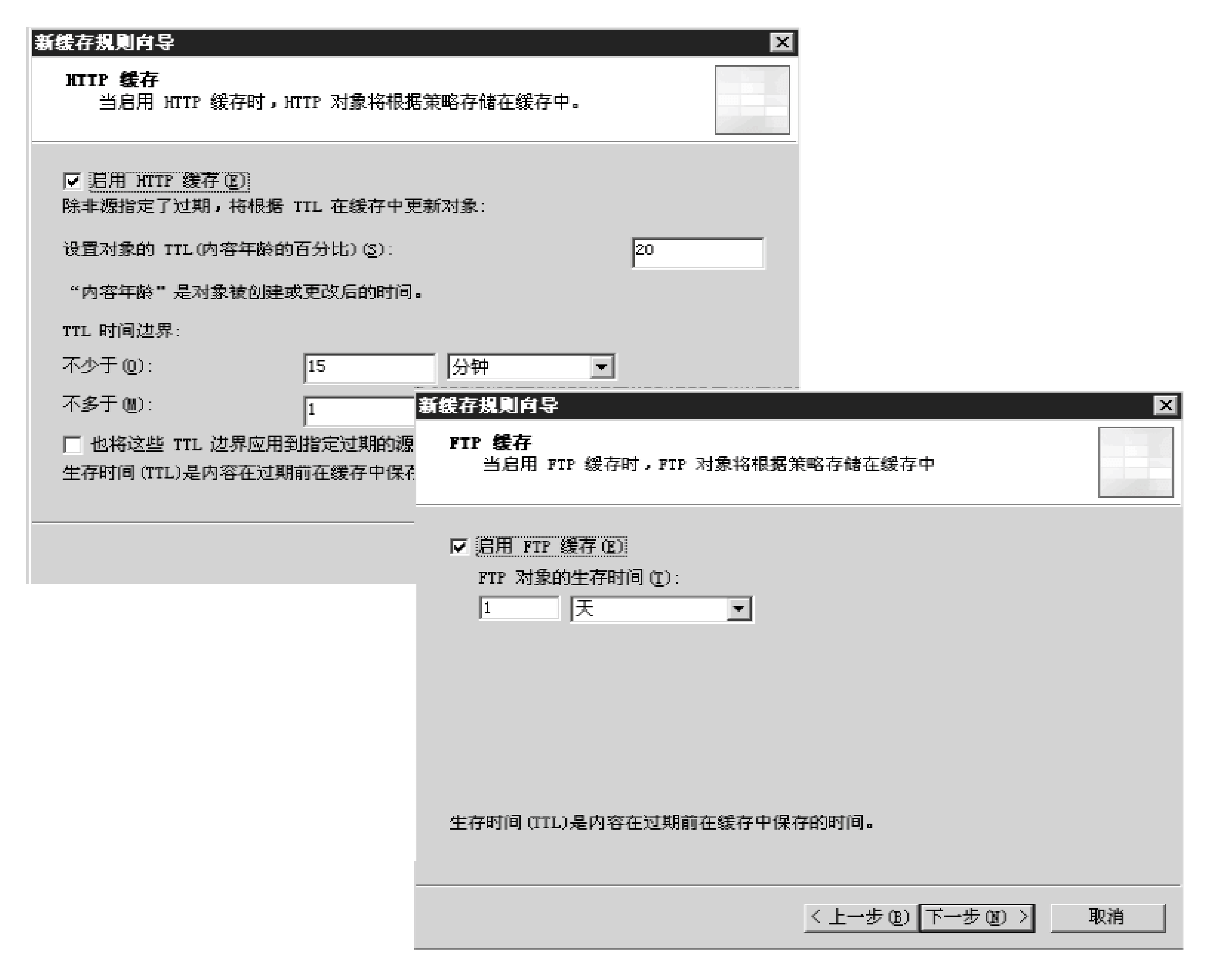


图 8-76　选择启用 HTTP 缓存和 FTP 缓存

❻ 完成新缓存规则向导后，检查设置是否正确，单击【完成】按钮。单击【应用】按钮保存修改和更新防火墙策略。这时 ISA Server 2004 会弹出一个提示框，选中【保存更改，并重启动服务】单选按钮，然后单击【确定】按钮即可。

8.5　Linux 防火墙

通常，Cisco PIX/ASA 和 Microsoft ISA Server 等解决方案的部署将使用大量的预算。对于一些刚刚起步的小型企业而言，使用这样的方案成本过于高昂，它们需要一种相对廉价的解决方案，基于 Linux 的防火墙是一个很好的选择。

8.5.1　Linux 防火墙简介

从 Linux 1.1 内核开始，Linux 就具有包过滤功能了，在 2.0 内核中采用 Ipfwadm 来操作内核包过滤规则。之后，在 2.2 内核中采用了大家并不陌生的 Ipchains 来控制内核包过虑规则。现在最新的 Linux 内核版本是 2.4.1，在 2.4 内核中不再使用 Ipchains，而是采用一个全新的内核包过滤管理工具——Iptables。这个全新的内核包过滤工具将使用户更易于理解其工作原理，更容易使用，当然也具有更为强大的功能。

Iptables 只是一个管理内核包过滤的工具，利用该工具可以加入、插入或删除核心包过滤表格(链)中的规则。实际上真正来执行这些过滤规则的是 Netfilter(Linux 核心中一个通用架构)及其相关模块(如 Iptables 模块和 NAT 模块)。下面介绍 Netfilter 的工作原理。

1. Netfilter 的工作原理

Netfilter 是 Linux 核心中一个通用架构，它提供了一系列的“表”，每个表由若干“链”组成，而每条链由一条或数条“规则”组成。可以这样来理解，Netfilter 是表的容器，表是链的容器，而链又是规则的容器。

系统默认的表为 Filter(过滤)，该表中包含了 INPUT(输入)、FORWARD(转发)和 OUTPUT(输出)三条链。每条链中可以有一条或数条规则，每条规则都是这样定义的：“如果数据包头符合这样的条件，就这样处理这个数据包”。当一条数据包到达一条链时，系统就会从第一条规则开始检查，看是否符合该规则所定义的条件，如果满足，系统将根据该条规则所定义的方法处理该数据包；如果不满足则继续检查下一条规则。最后，如果该数据包不符合该链中任意一条规则的话，系统就会根据该链预先定义的策略来处理该数据包。

当有数据包进入系统时，系统首先根据路由表决定将数据包发给哪条链。可能有三种情况。

- ✧ 如果数据包的目的地址是本机，则系统将数据包送往 INPUT 链，如果通过规则检查，则该包被发给相应的本地进程处理；如果没通过规则检查，系统就会将这个包丢掉。
- ✧ 如果数据包的目的地址不是本机，也就是说，这个包将被转发，则系统将数据包送往 FORWARD 链，如果通过规则检查，则该包被发给相应的本地进程处理；如果没通过规则检查，系统就会将这个包丢掉。
- ✧ 如果数据包是由本地系统进程产生的，则系统将其送往 OUTPUT 链，如果通过规则检查，则该包被发给相应的本地进程处理；如果没通过规则检查，系统就会将这个包丢掉。

图 8-77 说明了 Netfilter/Iptables 过滤数据包的过程。

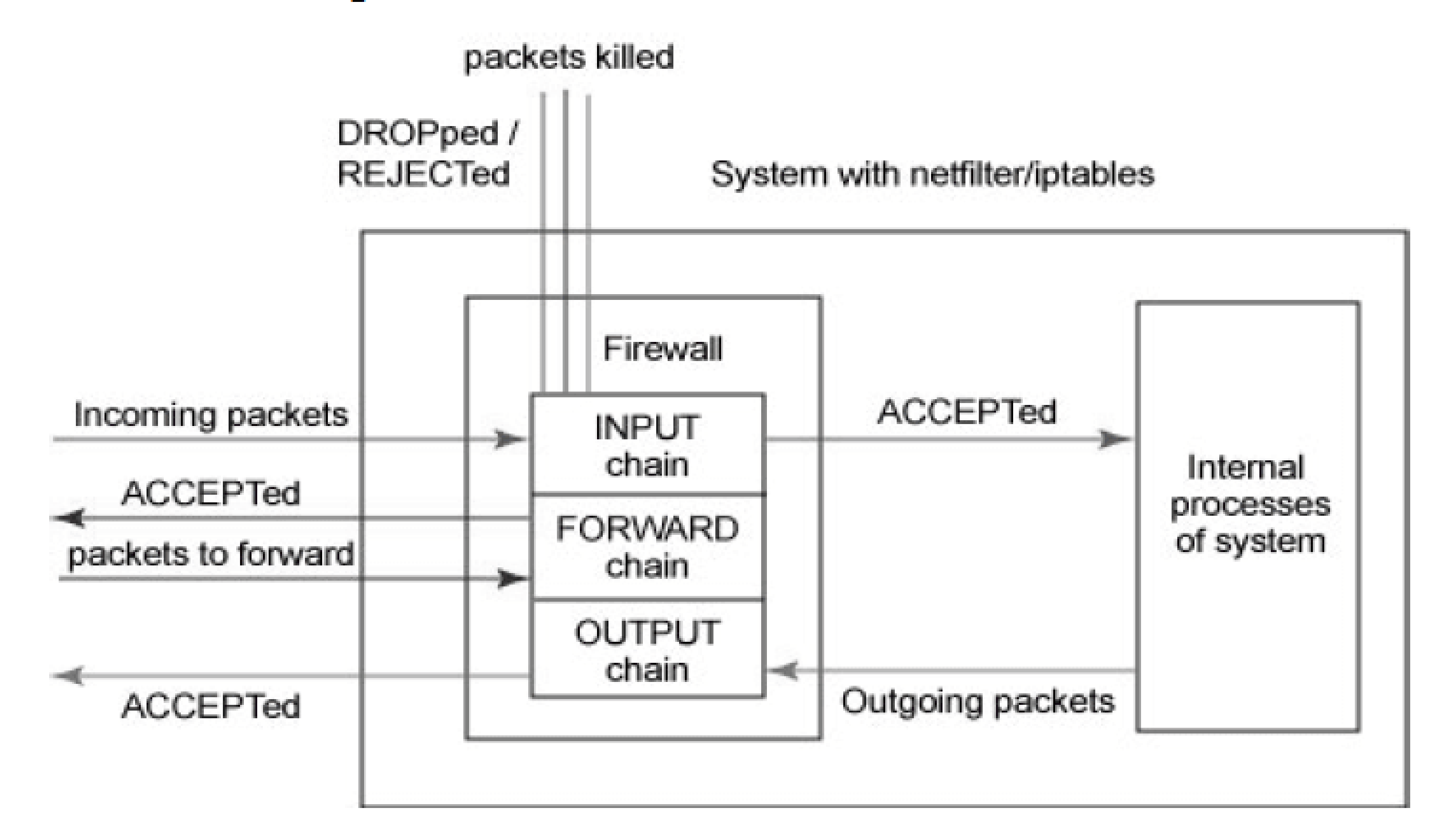


图 8-77　Netfilter/Iptables 过滤数据包的过程示意图

2. Netfilter 中的链和表

Netfilter 中有 5 种内置的链，这 5 种链可以组成 Filter、NAT 和 Mangle 三种不同的表。

1) Filter 表

Filter 表用来过滤数据包，可以在任何时候匹配包并过滤它们。我们就是在这里根据包的内容将包丢弃或接受的。当然，也可以预先在其他地方做些过滤，但是这个表才是设计用来过滤的。几乎所有的目标都可以在这个表中使用。Filter 表包括 Input、Forward 和 Output 等 3 种内置的链。

2) NAT 表

NAT 表主要实现地址转换功能，它包括 Prerouting、Postrouting、Output 等 3 种内置的链。NAT 表的操作分为 DNAT(目标网络地址转换)操作、SNAT(源网络地址转换)操作和 MASQUERADE(伪装)操作。

- ✧ DNAT 操作：该操作主要用于这样一种情况：有一个合法的 IP 地址，要把对防火墙的访问重定向到其他机器上(比如 DMZ)。也就是说，我们改变的是目的地址，使数据包能够路由到某台主机。
- ✧ SNAT 操作：该操作改变包的源地址，这在极大程度上可以隐藏本地网络细节或者 DMZ 等。一个很好的例子是我们知道防火墙的外部地址，但必须用这个地址替换本地网络地址。有了这个操作，防火墙就能自动地对包做 SNAT 和 De-SNAT(就是反向的 SNAT)操作，以使 LAN 能连接到 Internet。如果使用类似 192.168.0.0/24 这样的地址，是不会从 Internet 得到任何回应的。因为 IANA(Internet Assigned Numbers Authority，因特网号码分配管理局)定义这些网络(还有其他的)为私有的，只能用于 LAN 内部。
- ✧ MASQUERADE 操作：该操作的作用和 SNAT 完全一样，只是计算机的负荷稍微多一点。因为对每个匹配的包，MASQUERADE 都要查找可用的 IP 地址，而不像 SNAT 用的 IP 地址是配置好的。当然，这也有好处，就是我们可以使用通过 PPP、



PPPOE、SLIP 等拨号得到的地址，这些地址可是由 ISP 的 DHCP 随机分配的。

3)　Mangle 表

Mangle 表仅对数据包中的 TOS、TTL、MARK 字段进行操作。

✧ 对 TOS 的操作：用来设置或改变数据包的服务类型域，常用来设置网络上的数据包如何被路由等策略。注意，这个操作并不完善。它在 Internet 上还不能使用，而且很多路由器不会注意到这个域值。
✧ 对 TTL 的操作：用来改变数据包的生存时间域，我们可以让所有数据包只有一个特殊的 TTL。它的存在有一个很好的理由，那就是我们可以欺骗一些 ISP。为什么要欺骗它们呢？因为它们不愿意让我们共享一个连接。那些 ISP 会查找一台单独的计算机是否使用不同的 TTL，并且以此作为判断连接是否被共享的标志。
✧ 对 MARK 的操作：用来给包设置特殊的标记。IP Route 2 能识别这些标记，并根据不同的标记(或没有标记)决定不同的路由。使用这些标记我们可以做带宽限制和基于请求的分类。

8.5.2　配置 Linux 防火墙

利用 Linux 配置防火墙，通常设置两块网卡，一块流入，一块流出。Iptables 读取流入和流出的数据包的报头，然后将它们与规则集相比较，将可接受的数据包从一块网卡转发至另外一块网卡。对于被拒绝的数据包，可以被丢弃或者按照用户所定义的方式来处理。

通过向防火墙提供有关针对源 IP、目的 IP 或特定协议类型的信息包的规则，可以控制信息包的过滤。通过使用 Iptables 系统提供的特殊命令 Iptables 可以建立这些规则，并将其添加到内核空间的特定信息包过滤表内的链中。关于添加、除去、编辑规则的命令的一般语法如下。

```
Iptables [-t table] command [match] [target]
```

其中部分命令的含义如下。

✧ -t table：用来指定规则表。内建的规则表有 3 个，分别是：Nat、Mangle 和 Filter。当未指定规则表时，则一律视为 Filter。
✧ command：用来规则地进行操作，常用命令有-A(新增规则)、-D(删除一条规则)、-R(取代现行规则)、-I(插入一条规则)、-L(列出某规则链中的所有规则)、-F(删除某规则链中的所有规则)、-P(定义过滤政策，对未符合过滤条件的数据包预设的处理方式)等。
✧ match ：用来定义数据包的匹配方法，主要有--p(匹配数据包的协议类型，如 tcp、udp)、-s(匹配数据包的源 IP)、-d(匹配数据包的目的 IP)、-i(数据包进入的接口，如 eth0)、-o(数据包转发的接口，如-o eth1)、--sport(匹配数据包的源端口号)、--dport(匹配数据包的目的端口号)、--tcp-flags(匹配 TCP 数据包的状态标记，如--tcp-flags SYN,FIN,ACK SYN)、-m state --state(匹配数据包的连接状态，有 INVALID、ESTABLISHED、NEW 和 RELATED 四种)等。
✧ target：设置处理运作，通过-j 参数指定要进行的处理动作。常用的处理动作有

ACCEPT(放行数据包)、REJECT(拦阻数据包)、DROP(丢弃数据包不予处理)、REDIRECT(将数据包重新导向到另一个端口)、MASQUERADE(改写数据包来源 IP 为防火墙 NIC IP)、LOG(将数据包相关信息记录在 /var/log 中)、DNAT(改写数据包目的地 IP 为某特定 IP 或 IP 范围)、SNAT(改写数据包来源 IP 为某特定 IP 或 IP 范围)、MIRROR(镜像数据包，也就是将来源 IP 与目的 IP 对调后，将数据包送回)、QUEUE(中断过滤程序，将数据包放入队列，交给其他程序处理)、RETURN(结束在目前规则链中的过滤程序，返回主规则链继续过滤)、MARK(将数据包标上某个代号，以便提供作为后续过滤的条件判断依据)。

下面是一个常用的 Linux 防火墙的数据过滤脚本例子。

```
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
# iptables -A INPUT i lo j ACCEPT
# iptables -A INPUT -p tcp s 0.0.0.0/0 --dport 22 m state --state NEW -j ACCEPT
# iptables -A INPUT p tcp s 0.0.0.0/0 --dport 25 m state --state NEW -j ACCEPT
# iptables -A INPUT p tcp s 0.0.0.0/0 --dport 80 m state --state NEW -j ACCEPT
# iptables -A INPUT p tcp s 0.0.0.0/0 --dport 5900 m state --state NEW -j
ACCEPT
# iptables -A INPUT p tcp s 0.0.0.0/0 --dport 5901 m state --state NEW -j
ACCEPT
# iptables -A INPUT m state --state ESTABLISHED，RELATED -j ACCEPT
# iptables -A INPUT --reject-with icmp-host-prohibited -j REJECT
```

如果要防止 TCP SYN 攻击，可在脚本中增加如下一行。

```
# iptables -A FORWARD -p tcp --tcp-flags ALL SYN -j DROP
```

如果要防止 IP 碎片攻击，可在脚本中增加如下一行。

```
# iptables -A FORWARD -f -s 10.0.0.0/24 -d 192.168.1.1 -j DROP
```

可以通过限制 ICMP 报文频率来防范 ICMP 攻击，方法是在脚本中增加如下代码。

```
#iptables -A INPUT -p icmp -m limit --limit 6/m --limit-burst 5 -j ACCEPT
#iptables -P INPUT DROP
```

8.5.3 透明 Linux 防火墙

有时候，我们仅仅需要在两个网络之间实现访问控制，但又不想改动原本的网络结构，这时就需要用到透明防火墙。所谓透明防火墙，就是用户完全意识不到防火墙的存在，就像在两个网络中增加一台网桥(非透明的防火墙相当于一台路由器)，网络设备(包括主机、路由器、工作站等)和所有计算机的设置(包括 IP 地址和网关)无须改变，同时解析所有通过它的数据包，既增加了网络的安全性，又降低了用户管理的复杂程度。Linux 防火墙也可以实现透明模式，具体配置方法如下。

❶ 配置网络，使防火墙两块网卡均有相同的 IP 地址。配置方法是修改/etc/sysconfig/network-scripts/ifcfg-eth0 和/etc/sysconfig/network-scripts/ifcfg-eth1 两个文件，使其文件内容如下。

```
DEVICE=eth0
```

```
BOOTPROTO=none
BROADCAST=10.17.74.255
IPADDR=10.17.74.254
NETMASK=255.255.255.0
NETWORK=10.17.74.0
ONBOOT=yes
USERCTL=no
PEERDNS=no
TYPE=Ethernet DEVICE=eth1
BOOTPROTO=none
BROADCAST=10.17.74.255
IPADDR=10.17.74.254
NETMASK=255.255.255.0
NETWORK=10.17.74.0
ONBOOT=yes
USERCTL=no
PEERDNS=no
TYPE=Ethernet
```

❷ 在文件 /etc/sysconfig/network-scripts/ifcfg-eth0 中加入一行用来设置默认路由。

```
gateway=10.17.74.1
```

❸ 执行如下命令启用数据包转发和 ARP 代理(Proxy_arp)功能。

```
#Ip forward
/sbin/sysctl -w net.ipv4.conf.all.forwarding=1
#Enable proxy-arp
/sbin/sysctl -w net.ipv4.conf.eth0.proxy_arp=1
/sbin/sysctl -w net.ipv4.conf.eth1.proxy_arp=1
```

❹ 由于两块网卡(eth0、eth1)使用同样的 IP，如果不指定转发路径，会导致路由混乱，从而使防火墙内的计算机无法访问 Internet。指定转发路径的方法是在 /etc/rc.d/rc.local 文件中添加如下几行。

```
#Define route
/sbin/ip route del 10.17.74.0/24 dev eth0
/sbin/ip route add 10.17.74.1 dev eth0
/sbin/ip route add 10.17.74.0/24 dev eth1
```

❺ 配置完成后，运行 service network restart 命令重新启动网络服务或重新启动计算机，使配置生效。

8.5.4　管理 Linux 防火墙

如果仅通过命令行来管理 Linux 防火墙，维护起来比较困难。如果在 Linux 防火墙上安装并配置 Webmin，用户就可以与 Cisco ASDM 一样，可以使用图形的管理方式来管理防火墙了。下面简要介绍其配置过程。

❶ 安装 Webmin 后，在服务器上通过http://127.0.0.1:10000访问，并输入用户名 root 及密码，如图 8-78 所示。登录 Webmin 后，可以将界面转换为中文。

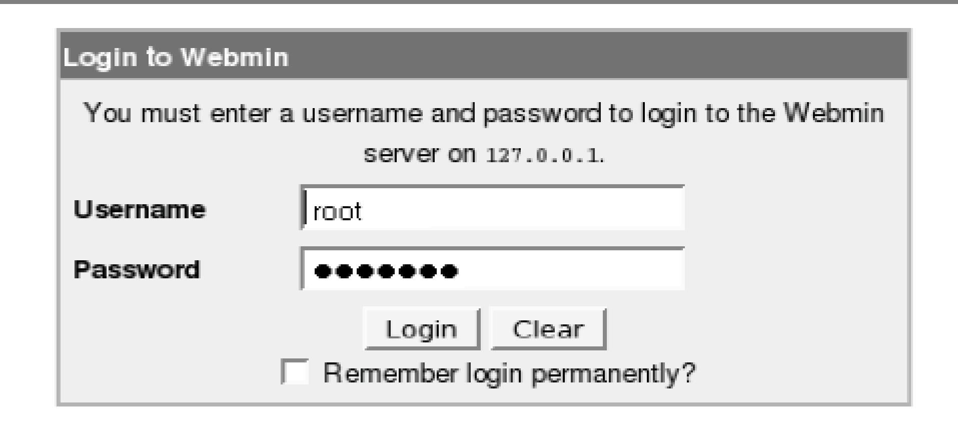


图 8-78　登录 Webmin

❷ 登录成功后，进入 Webmin 的配置界面，选择【网络】→Linux Firewall 结点，如图 8-79 所示。

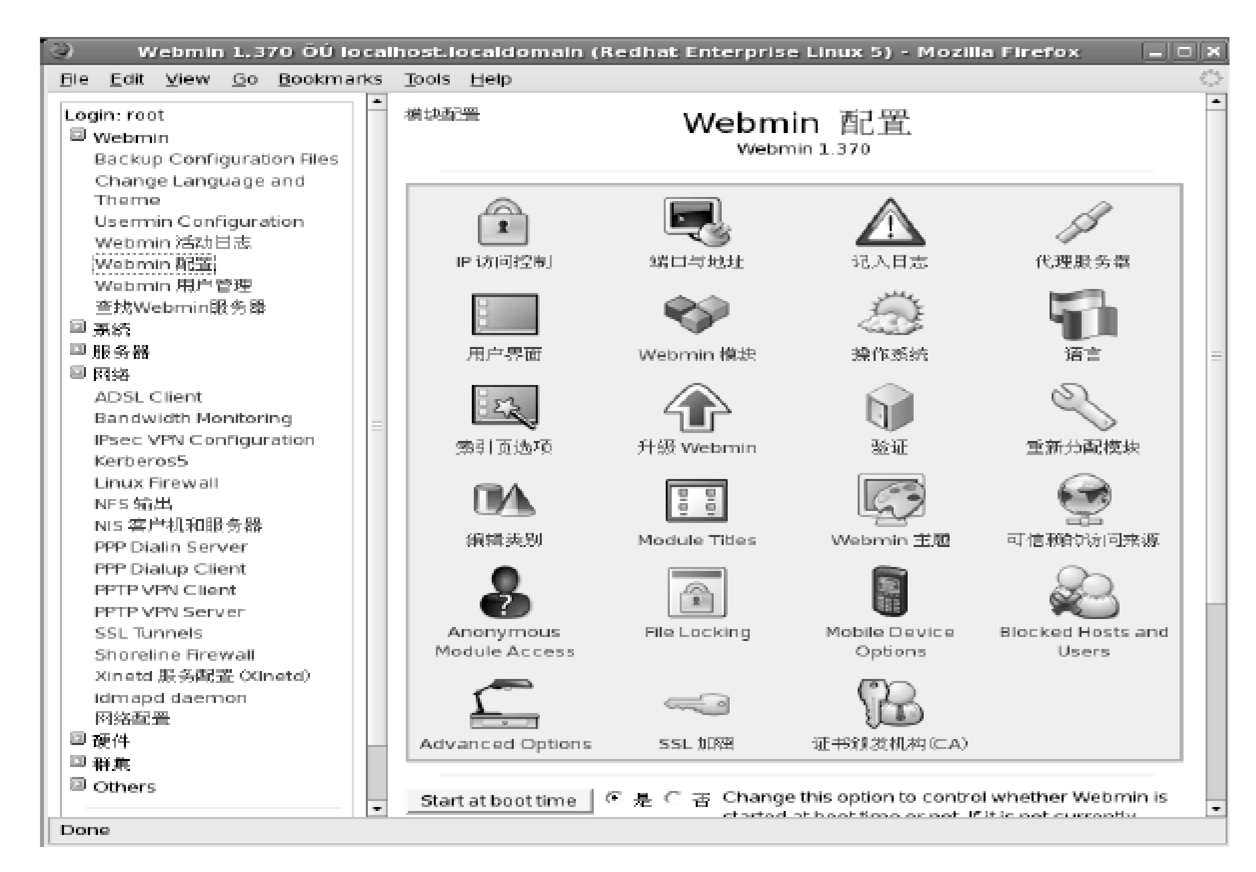


图 8-79　Webmin 配置界面

❸ 进入 Linux Firewall 配置界面后，可以看到 Linux 默认的 3 种表(Filter、Mangle 和 NAT)，如图 8-80 所示。

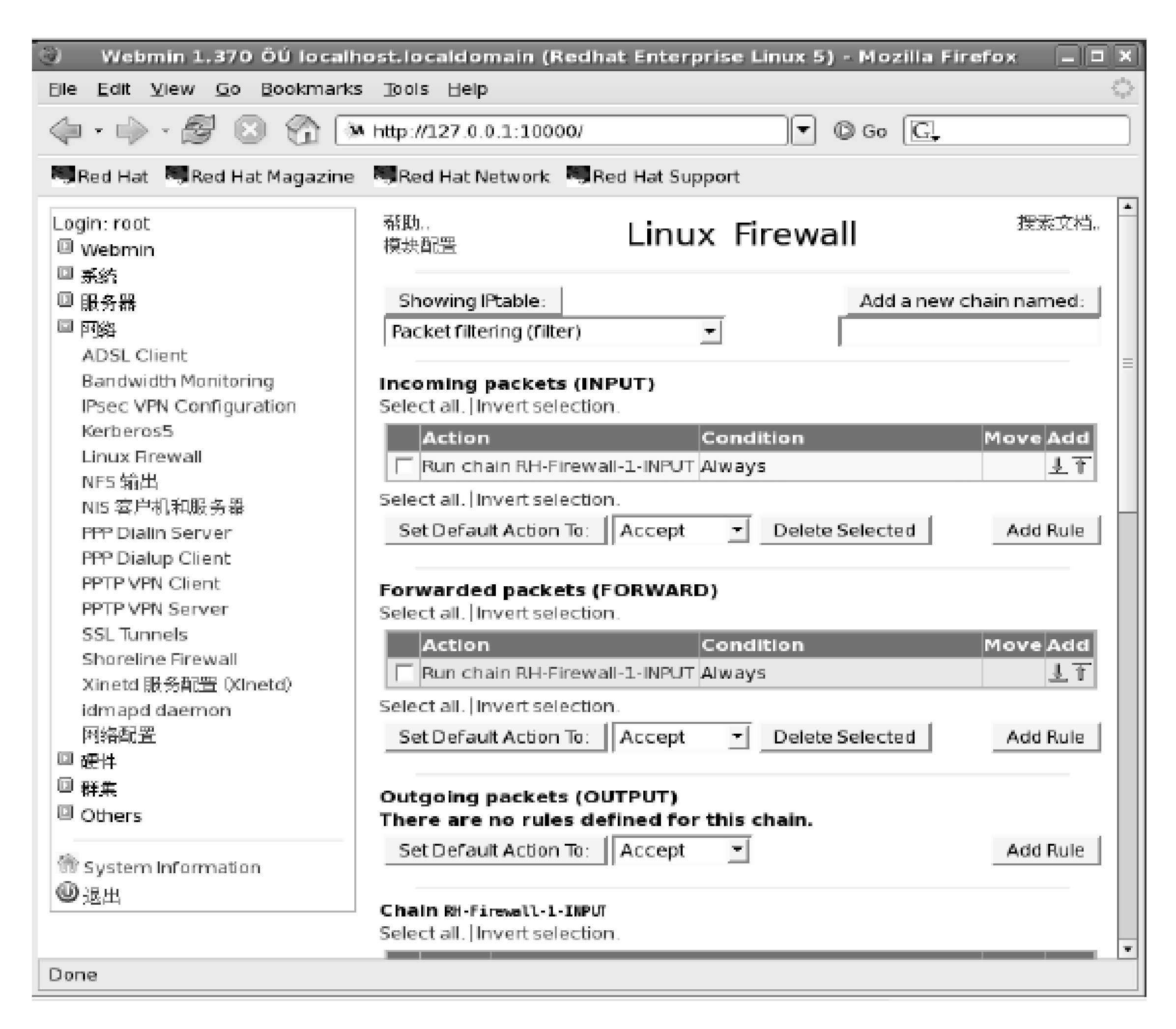


图 8-80　Linux Firewall 配置界面

❹ 单击其中一个表，可以看到该表的访问规则，图 8-81 所示的是 Filter 表。

	Action	Condition	Move	Add
☐	Accept	If input interface is **lo**		
☐	Accept	If protocol is **ICMP** and ICMP type is **any**		
☐	Accept	If protocol is **50**		
☐	Accept	If protocol is **51**		
☐	Accept	If protocol is **UDP** and destination is **224.0.0.251** and destination port is **5353**		
☐	Accept	If protocol is **UDP** and destination port is **631**		
☐	Accept	If protocol is **TCP** and destination port is **631**		
☐	Accept	If state of connection is **ESTABLISHED,RELATED**		
☐	Accept	If protocol is **TCP** and destination port is **21** and state of connection is **NEW**		
☐	Accept	If protocol is **TCP** and destination port is **25** and state of connection is **NEW**		
☐	Accept	If protocol is **TCP** and destination port is **22** and state of connection is **NEW**		
☐	Accept	If protocol is **TCP** and destination port is **443** and state of connection is **NEW**		
☐	Accept	If protocol is **TCP** and destination port is **23** and state of connection is **NEW**		
☐	Accept	If protocol is **TCP** and destination port is **80** and state of connection is **NEW**		
☐	Reject	Always		

图 8-81　Filter 表

❺ 在图 8-81 中，可以单击 Add Rule 按钮，进行规则的添加和删除等操作。

8.6　本章小结

本章介绍了 Cisco IOS Firewall、PIX/ASA、微软 ISA Server 2004 和 Linux Iptables 等多种防火墙系统。Cisco IOS Firewall 主要针对原来已经部署 IOS 路由器的用户，目的是获得安全性的提升。ASA 是 Cisco 推出的具有代表性的 UTM 产品，通过一个设备实现了防火墙、防病毒网关、邮件过滤网关、VPN 服务器、IPS 入侵检测等众多功能，这样的产品对于提升网络安全性具有很大的帮助。微软 ISA Server 2004 主要用于使用一些低端路由器、交换机平台(这些产品上没有足够的安全选项)，并已经部署了大量的 Windows 系统的公司。Linux 防火墙由于是一个免费系统，可以获得较好的安全性，并且通过 Web 的方式也容易配置。

第 9 章　入侵检测及防御

随着网络安全风险系数不断提高，曾经作为最主要的安全防范手段的防火墙，已经不能满足人们对网络安全的需求。作为对防火墙极其有益的补充，IDS(Intrusion Detection Systems，入侵检测系统)能够帮助网络系统快速发现攻击的发生，它扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。与此同时，互联网中 DDoS 攻击等入侵行为使用频率越来越高，如何有效地防御 DDoS 攻击也是维护网络安全的重要任务。

通过本章的学习，读者应掌握以下主要内容：

✧ IPS/IDS 工作原理
✧ 常见 IPS、IDS 系统配置方式
✧ Linux IDS 实现
✧ DDoS 防御

9.1　IPS/IDS 工作原理

9.1.1　IDS 工作原理

本质上，入侵检测系统是一个典型的“窥探设备”，它不能跨接多个物理网段(通常只有一个监听端口)，无须转发任何流量，而只需要在网络上被动地、无声息地收集它所关心的报文即可。IDS 处理过程分为数据采集阶段、数据处理及过滤阶段、入侵分析及检测阶段、报告及响应阶段等 4 个阶段。在数据采集阶段中，入侵检测系统收集目标系统中引擎提供的主机通信数据包和系统使用等情况；数据处理及过滤阶段是把采集到的数据转换为可以识别是否发生入侵的阶段；入侵分析及检测阶段通过分析上一阶段提供的数据来判断是否发生入侵，这一阶段是整个入侵检测系统的核心阶段，根据系统是以检测异常使用为目的还是以检测利用系统的脆弱点或应用程序的 BUG 来进行入侵为目的，可以区分为异常行为和错误使用检测；报告及响应阶段针对上一个阶段中进行的判断作出响应，如果判断为发生入侵，系统将对其采取相应的响应措施，或者通知管理人员发生入侵，以便于采取措施。最近人们对入侵检测及响应的要求日益增加，特别是对其跟踪功能的要求越来越强烈。

目前，IDS 分析及入侵检测阶段一般通过以下几种技术手段进行分析：特征码匹配、基于统计分析和完整性分析。其中，前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

特征库匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，

从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令)，也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般来讲，一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

统计分析方法首先给信息对象(如用户、连接、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常偏差之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚 8 点至早 6 点不登录的账户却在凌晨 2 点试图登录，或者针对某一特定站点的数据流量异常增大等。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。

完整性分析主要关注某个文件或对象是否被更改，包括文件和目录的内容及属性，它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数(如 MD5)，能识别极其微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不用于实时响应。

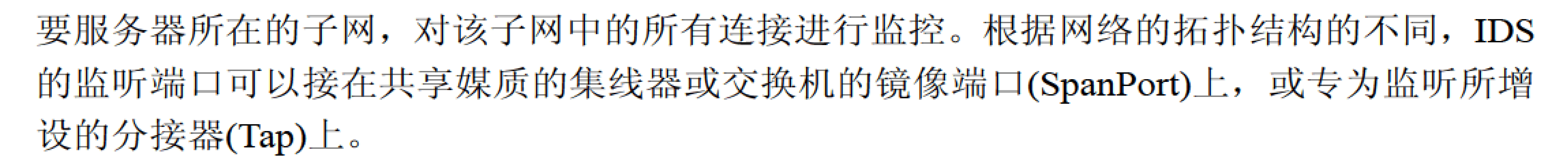
9.1.2　部署 IDS

防火墙在网络安全中起到大门警卫的作用，对进出的数据依照预先设定的规则进行匹配，符合规则的就予以放行，起访问控制的作用，是网络安全的第一道闸门。优秀的防火墙甚至对高层的应用协议进行动态分析，保护进出数据应用层的安全。但防火墙的功能也有局限性，防火墙只能对进出网络的数据进行分析，对网络内部发生的事件完全无能为。同时，由于防火墙处于网关的位置，不可能对进出攻击做太多判断，否则会严重影响网络性能。

如果把防火墙比作大门警卫的话，IDS 就是网络中不间断的摄像机。在实际的部署中，IDS 是并联在网络中，通过旁路监听的方式实时地监视网络中的流量，对网络的运行和性能无任何影响，同时判断其中是否含有攻击的企图，通过各种手段向管理员报警，不但可以发现外部的攻击，也可以发现内部的恶意行为。所以说，IDS 是网络安全的第二道闸门，是防火墙的必要补充，可构成完整的网络安全解决方案。

严格地说，IDS 并不是一个防范工具，它并不能阻断攻击。只有防火墙才能限制非授权的访问，在一定程度上防止入侵行为。而 IDS 提供快速响应机制，报告入侵行为，意味着一种牵制政策。IDS 可以与防火墙在功能上实现联动，进行很好地配合，将大大提高网络系统的安全性。当 IDS 检测到入侵行为发生，立即发出一个指令给防火墙，防火墙马上关闭通信连接，从而阻断入侵。

目前，大部分的 IDS 产品基本上由入侵检测引擎和管理控制台组成，在具体应用时可以根据网络结构和需求做不同的部署。一般都部署在需要重点保护的部位，如企业内部重



要服务器所在的子网，对该子网中的所有连接进行监控。根据网络的拓扑结构的不同，IDS 的监听端口可以接在共享媒质的集线器或交换机的镜像端口(SpanPort)上，或专为监听所增设的分接器(Tap)上。

9.1.3　IPS 与 IDS 的区别

早期的 IDS 通过查找任何异常的通信发挥作用。当检测到异常的通信时，这种行为将被记录下来并且向管理员发出警报。这个过程很少出现问题。对于初始者来说，查找异常通信方式会产生很多错误的报告。经过一段时间之后，管理员会对收到过多的错误警报感到厌烦，从而完全忽略 IDS 的警报。

IDS 的另一个主要缺陷是它们仅监视主要的通信。如果检测到一种攻击，它将提醒管理员采取行动。人们认为 IDS 采取的这种方法是很好的。总之，由于 IDS 会产生很多的错误报告，用户真的愿意让 IDS 对合法的网络通信采取行动吗?

在过去的几年里，IDS 已经有了很大的进步。目前，IDS 的工作方式更像是一种杀毒软件。IDS 包含一个名为攻击特征的数据库。这个系统不断地把入网的通信与数据库中的信息进行比较。如果检测到攻击行动，IDS 就发出这个攻击的警报。

比较新的 IDS 比以前的系统更准确一些。但是，这个数据库需要不断地更新以保持有效性。而且，如果发生了攻击并且在数据库中没有相匹配的特征，这个攻击可能就会被忽略。即使这个攻击被检测到并且被证实是一种攻击，IDS 除了向管理员发出警报和记录这个攻击之外没有力量做任何事情。这就是入侵防御系统(IPS)的任务了。IPS 与 IDS 类似，但是 IPS 在设计上解决了 IDS 的一些缺陷。

对于初始者来说，IPS 位于防火墙和网络设备之间。这样，如果检测到攻击，IPS 会在这种攻击扩散到网络的其他地方之前阻止这个恶意的通信。相比之下，IDS 只是存在于网络之外起到报警的作用，而不是在网络前面起到防御的作用。

IPS 检测攻击的方法也与 IDS 不同。目前有很多种 IPS 系统，它们使用的技术都不相同。但是，一般来说，IPS 系统都依靠对数据包的检测。IPS 通过检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入网络。

9.1.4　IPS 简介

IPS 实现实时检查和阻止入侵的原理在于拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。IPS 数据包处理引擎是专业化定制的集成电路，可以深层检查数据包的内容。如果有攻击者利用 Layer 2 (介质访问控制)至 Layer 7(应用)的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对 Layer 3 或 Layer 4 进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐字节地检查数据包。所有流经 IPS 的数据包都被分类，分类的依据是数据包中的报头信息，例如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续通行，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一

步的检查。

针对不同的攻击行为，IPS 需要不同的过滤器。每种过滤器都设有相应的过滤规则，为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤器引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤准确性。

过滤器引擎集合了流水线和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。这种硬件加速技术对于 IPS 具有重要意义，因为传统的软件解决方案必须串行进行过滤检查，会导致系统性能大打折扣。

1. 基于主机的入侵防护(HIPS)

HIPS 通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防护能够保护服务器的安全弱点不被不法分子所利用。Cisco 公司的 Okena、NAI 公司的 McAfee Entercept、冠群金辰的龙渊服务器核心防护都属于这类产品，它们在防范红色代码和 Nimda 的攻击中起到了很好的防护作用。基于主机的入侵防护技术可以根据自定义的安全策略以及分析学习机制来阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺取控制权的入侵行为，整体提升主机的安全水平。

在技术上，HIPS 采用独特的服务器保护途径，利用由包过滤、状态包检测和实时入侵检测组成的分层防护体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，既可以以软件形式嵌入到应用程序对操作系统的调用当中，通过拦截针对操作系统的可疑调用，提供对主机的安全防护；也可以以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。

由于 HIPS 工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用和资源的未授权的任何非法访问。HIPS 与具体的主机/服务器操作系统平台紧密相关，不同的平台需要不同的软件代理程序。

2. 基于网络的入侵防护(NIPS)

NIPS 通过检测流经的网络流量，提供对网络系统的安全保护。由于它采用在线连接方式，所以一旦辨识出入侵行为，NIPS 就可以去除整个网络会话，而不仅仅是复位会话。同样由于实时在线，NIPS 需要具备很高的性能，以免成为网络的瓶颈，因此 NIPS 通常被设计成类似于交换机的网络设备，提供线速吞吐速率以及多个网络端口。

NIPS 必须基于特定的硬件平台，才能实现千兆级网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为 3 类：网络处理器(网络芯片)、专用的 FPGA 编程芯片和专用的 ASIC 芯片。

在技术上，NIPS 吸取了目前 NIPS 所有的成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是最广泛应用的技术，具有准确率高、速度快的特点。基于状态的特征匹配不但检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。

3. 应用入侵防护(AIP)

NIPS 产品有一个特例，即应用入侵防护(Application Intrusion Prevention，AIP)，它把基于主机的入侵防护扩展成为位于应用服务器之前的网络设备。AIP 被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设置好的安全策略，保护服务器的安全。NIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

NIPS 的实时检测与阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。

IPS 技术需要面对很多挑战，其中主要有 3 点：一是单点故障，二是性能瓶颈，三是误报和漏报。设计要求 IPS 必须以嵌入模式工作在网络中，而这就可能造成瓶颈问题或单点故障。如果 IDS 出现故障，最坏的情况也就是造成某些攻击无法被检测到，而嵌入式的 IPS 设备出现问题，就会严重影响网络的正常运转。如果 IPS 出现故障而关闭，用户就会面对一个由 IPS 造成的拒绝服务问题，所有客户都将无法访问企业网络提供的应用。

即使 IPS 设备不出现故障，它仍然是一个潜在的网络瓶颈，不仅会增加滞后时间，而且会降低网络的效率，IPS 必须与数千兆或者更大容量的网络流量保持同步，尤其是当加载了数量庞大的检测特征库时，设计不够完善的 IPS 嵌入设备将无法支持这种响应速度。绝大多数高端 IPS 产品供应商都通过使用自定义硬件(FPGA、网络处理器和 ASIC 芯片)来提高 IPS 的运行效率。

误报率和漏报率也需要 IPS 认真面对。在繁忙的网络当中，如果以每秒需要处理十条警报信息来计算，IPS 每小时至少需要处理 36 000 条警报，一天就是 864 000 条。一旦生成了警报，最基本的要求就是 IPS 能够对警报进行有效处理。如果入侵特征编写得不是十分完善，那么“误报”就有了可乘之机，导致合法流量也有可能被意外拦截。对于实时在线的 IPS 来说，一旦拦截了攻击性数据包，就会对来自可疑攻击者的所有数据流进行拦截。如果触发了误报警报的流量恰好是某个客户订单的一部分，其结果可想而知。

9.1.5　常见 IPS 产品

随着互联网络的发展，众多 IPS 产品问世，其中具有代表性的产品有 ISS Proventia、Cisco IPS/IDS 解决方案、BLADE IDS Informer 测试仪，等等。

1. ISS Proventia

Internet Security Systems 公司的 Proventia G 系列是串接式入侵防护系统，能够在保持网络带宽及可用性的同时自动阻断恶意的攻击。Proventia G 系列设备(如图 9-1 所示)在准确性与防护能力方面，大大超过了现有的防火墙、入侵检测系统以及其他串接式入侵防护系统产品。作为先进的串接式入侵防护系统，Proventia G 系列硬件设备能够实时阻断已知和未知的攻击，包括分布式拒绝服务(DDoS)、后门以及混合威胁等，而无须工作繁忙的系统管理人员的参与。

2. Cisco IPS/IDS 解决方案

Cisco 提供了一套完整的 IPS/IDS 解决方案。在 Cisco IOS 软件平台上，Cisco 提供了一种简单的 IPS 系统，用于基本的入侵过滤，并且 IPS 特性不会导致路由器性能下降。同时，Cisco 还支持网络型 IPS/IDS 平台(NIPS)，例如 Cisco IPS 4200 系列产品，如图 9-2 所示。在主机 IPS/IDS 平台(HIPS)中，Cisco 提供了基于 CSA 的安全代理平台。同时随着 ASA 系列集成了 IPS，Cisco 可以提供出色的 UTM 支持。



图 9-1　ISS Proventia G 系列产品

图 9-2　Cisco IPS 入侵防御系统

对于 IDS、IPS 产生的 Alarm 等日志信息，Cisco 可以通过 CS-MARS 管理所有的日志。

3. BLADE IDS Informer 测试仪

BLADE 公司推出的 IDS Informer 是第一个能够实现在生产环境中对 IDS/IPS 的布局、配置、策略的应用等进行测试的产品。

IDS Informer 采用在实验中针对每一种攻击，完整准确地录制真实攻击过程的网络数据包，再经过封装，自动化处理，形成一个攻击文件(.dll)，由此构建了一个庞大的攻击库来对 IDS/IPS 的各种攻击识别策略进行检测。它采用 SAFE 的专利技术，产生的是无害的网络流量，在网络中发送的是真实而安全的攻击数据包，因此不需要专门去准备攻击的目标系统。

IDS Informer 拥有 600 多种攻击类型，运行每一种攻击只需轻轻一点，几秒钟就可以完成。使用 IDS Informer，不需要对系统平台和编程技术有太多的了解，也不需要专门准备攻击目标系统。

9.2　配置 Cisco IPS/IDS

9.2.1　配置基于 Cisco IOS IPS/IDS

从 12.0(5)T 开始 IOS 已经开始支持 IDS 了，但是当时只支持 59 个特征码，并且可扩展性也很差，只能算个摆设而已。在 12.3(11)T 的 IPS 中支持 118 个特征码，并且最重要的是客户可以通过更新路由器上 Flash 的一个 SDF(Signature Definition File，特征码定义文件)来增加新的特征，通过新的设计，IPS 特性不会影响路由器的性能。

1. 配置 Cisco IOS IDS

Cisco IOS IDS 的大多数配置方法与 Cisco 路由器一样，下面简单地介绍一下对一台新

Cisco IOS IDS 的配置过程。

❶ 对 IDS 进行初始化，方法如下。

```
Router(config)# ip audit po max-events events_num
Router(config)# ip audit smtp spam recipients_num
```

❷ Cisco IOS 提供基于 Syslog 的服务来存储 IDS 的事件日志，配置如下。

```
Router(config)# ip audit notify log
```

❸ 为 IDS 设置事件行为。

```
Router(config)# ip audit info {action [alarm] [drop] [reset]}
Router(config)# ip audit attack {action [alarm] [drop] [reset]}
```

❹ 构建 IDS 列表，并设置相应的特征行为。

```
Router(config)# ip audit name SadnessIDS info action alarm
Router(config)# ip audit name SadnessIDS attack action alarm drop reset
Router(config)# ip audit signature signature_num disable
```

❺ 将 IDS 列表应用到某个网络端口上。

```
Router(config)# interface FastEthernet0/1
Router(config-if)# ip audit SadnessIDS in
```

❻ 下面是一个完整的 IDS 配置实例。

```
//定义IDS日志使用Syslog并定义IDS列表
Router(config)# ip audit notify log
Router(config)# ip audit name SadnessIDS info action alarm
Router(config)# ip audit name SadnessIDS attack action alarm drop reset
//关闭一些常见的特征，减少误报
Router(config)# ip audit signature 2000 disable   //ping
Router(config)# ip audit signature 2001 disable   //主机不可达
Router(config)# ip audit signature 2004 disable   //ping request
Router(config)# ip audit signature 2005 disable   //超时
Router(config)# ip audit signature 6051 disable   //DNS zone转换
//将配置应用到接口
Router(config)# interface FastEthernet1
Router(config-if)# ip audit SadnessIDS in
```

2. 配置 Cisco IOS IPS

对于 Cisco IOS IPS，它的配置过程如下。

❶ 在 Cisco 官方网站下载最新 SDF 文件，并在 IOS 中定义其位置。SDF 文件可以存放在设备的 Flash 中，也可以存放在一台 FTTP 服务器中。

```
Router(config)#ip ips sdf location tftp://10.0.0.1/ips.sdf
Router(config)#ip ips sdf location flash://ips/sigsdf
```

❷ 配置特征自动升级。

```
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# username cisco password cisco
Router(config-ips-auto-update)# url tftp://10.0.0.1/ipsautoupdate.xml
```

❸ 配置 IPS 列表，以关闭一些常见的特征，减少误报。

```
Router(config)#ip ips name sadness
Router(config)#ip ips signature 1107 0 disable
Router(config)#ip ips signature 3301 0 disable
Router(config)#ip ips signature 3051 0 disable
Router(config)#ip ips signature 3051 1 disable
```

4. 配置 IOS IPS 通过 SDEE 方式发送消息。

```
Router(config)# ip ips notify SDEE
Router(config)# ip sdee event 500
Router(config)# ip sdee subscriptions 1
Router(config)# ip sdee messages 500
Router(config)# ip sdee alerts 2000
```

5. 在设备端口上应用 IPS 列表。

```
Router(config)# interface FastEthernet1
Router(config-if)# ip ips sadness in
```

3. 在 Cisco PIX/ASA 上配置 IPS/IDS 功能

Cisco PIX/ASA 也可以在配置防火墙的基础上，再配置 IPS/IDS 功能。特别是 ASA 在安装 CSC-SSM 模块后，无法继续安装 AIP 模块时，可以按照下述方法来配置(注：PIX ware 7.2 版本)。

```
pixfirewall(config)#  ip audit name sadness attack action alarm drop reset
pixfirewall(config)#  ip audit name sadness2 info action alarm
pixfirewall(config)#  ip audit attack action alarm drop reset
pixfirewall(config)#  ip audit attack action alarm drop reset
pixfirewall(config)#  ip audit signature 2000 disable
pixfirewall(config)#  ip audit signature 2000 disable
pixfirewall(config)#  ip audit signature 2001 disable
pixfirewall(config)#  ip audit signature 2004 disable
pixfirewall(config)#  ip audit signature 2005 disable
pixfirewall(config)#  ip audit signature 6051 disable
pixfirewall(config)#  interface FastEthernet 0
pixfirewall(config-if)#  ip audit interface outside sadness
pixfirewall(config-if)#  ip audit interface outside sadness2
```

9.2.2 配置 Cisco NM-CIDS

Cisco 入侵检测网络模块(NM-CIDS)可以与 Cisco 接入路由器搭配来强化网络边界的安全，如图 9-3 所示。NM-CIDS 模块配置简单，可以与网络设备进行联动，配合 ISR 路由器 IOS IPS 功能可以使设备识别攻击、拦截攻击的能力大幅度强化。同时，利用 NM-CIDS 的信息发送给 IPS 网管软件 IEV(IDS Event Viewer，IDS 事件浏览器)或 Cisco 的安全网管 MARS，这样就可以更加有效地帮助网络管理员在网络边界有效地隔离攻击时间，同时了解网络的威胁。

但是，NM-CIDS 只能工作在 IDS 模式，并且不支持桥接接口。当检测到恶意行为穿过路由器时，NM-CIDS 可以和网络设备联动发送动态 ACL 实现连接复位等操作。

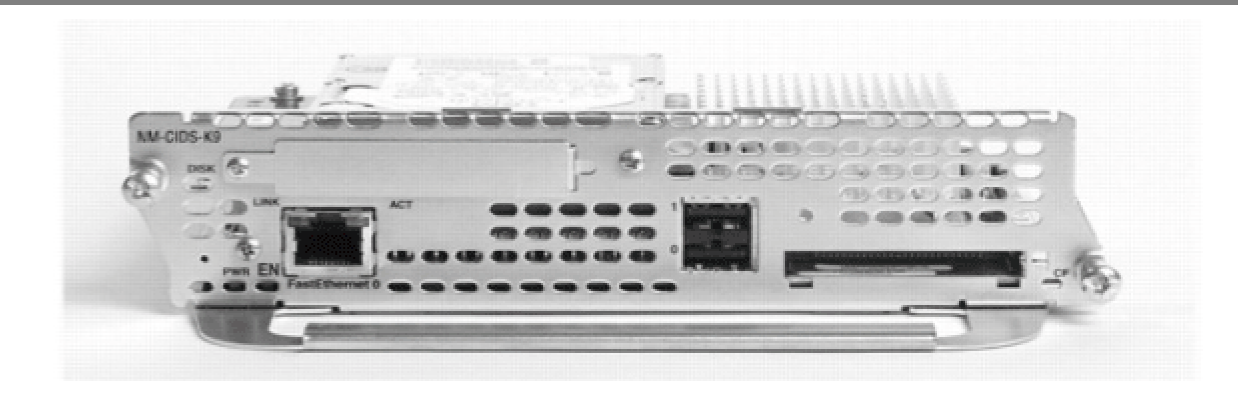


图 9-3　Cisco NM-CIDS

Cisco NM-CIDS 的配置主要包括模块的初始化、监控流量的导入，以及工作模式的配置等。

1. 初始化 NM-CIDS

对于一台新的 Cisco 入侵检测网络模块，在使用之前，需要对其进行初始化。下面简要地介绍一下初始化 NM-CIDS 的过程。

❶ 为加快数据转发速率，首先需要开启路由器 CEF 功能。

```
Router(config)#ip cef
```

❷ 接着，需要为 NM-CIDS Sensor 接口指定 IP 地址。

```
Router(config)# interface ids-sensor 1/0
Router(config-if)# ip unnumbered loopback 0
Router(config-if)# no shutdown
```

❸ 接下来，需要登录到路由器的 NM-CIDS Sensor 模块。

```
Router# service-module ids-sensor 1/0 session
```

❹ 登录到 NM-CIDS Sensor 模块后，为 NM-CIDS 配置管理接口，包括 IP 地址、网关、登录控制等。

```
sensor(config)# service host
sensor(config-hos-net)#network-settings
sensor(config-hos-net)#host-ip 192.168.1.200/24, 192.168.1.1
                                          //配置管理接口Ip地址和网关
sensor(config-hos-net)#host-name nm-cids
sensor(config-hos-net)#telnet-option enabled      //开启telnet选项
sensor(config-hos-net)#access-list 192.168.1.0/24    //配置管理地址网段
sensor(config-hos-net)#exit
```

❺ 最后还需要配置 NM-CIDS 时区。配置完成后，重新启动使配置生效。

```
sensor(config-hos)#time-zone-settings
sensor(config-hos-tim)#offset 8
sensor(config-hos-tim)#standard-time-zone-name beijing
sensor(config-hos-tim)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]:yes
Warning : Reboot is required before the configuration change will take effect
Warning : The node must be rebooted for the changes to go into effect.
Continue with reboot?[yes]:yes
```

❻ 重启完成后，还需要配置 Web 服务，用于 IDM 和 IEV 访问。

```
sensor(config)# service web-server
```

```
sensor(config-web)# enable-tls true
sensor(config-web)# port 443
sensor(config-web)# exit
Apply Changes:?[yes]: yes
```

2. 初始化 AIP 模块

ASA 所支持的 AIP 模块，同时支持按照 NM-CIDS 方式进行的初始化，还可以使用 setup 脚本进行配置，前一种初始化的配置在第 8 章已经介绍过，这里我们使用 setup 脚本配置。

```
sensor# setup
    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog?[yes]: yes
Enter host name[ssm_sensor]: ssm-sensor
Enter IP interface[10.0.0.2/24, 10.0.0.1]: 192.168.1.250/24, 192.168.1.1
Enter telnet-server status[disabled]: enabled
Enter web-server port[443]:443
Modify current access list?[no]: yes
Current access list entries:
Permit:192.168.1.0
Modify system clock settings?[no]: yes
  Use NTP?[no]: no
  Modify summer time settings?[no]: no
  Modify system timezone?[no]: yes
    Timezone[beijing]: beijing
    UTC Offset[8]: 8
Modify virtual sensor "vs0" configuration?[no]:

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
Enter your selection[2]: 2
Configuration Saved.
sensor#  reset
Warning:Executing this command will stop all applications and reboot the node.
Continue with reset? [] : yes
```

3. 初始化 IPS/IDS 4200 和 IDSM-2 模块

IDSM-2 模块相当于把 IPS 功能直接集成到交换机的线卡中，并从交换机背板中获得数据流，由此在 Catalyst 6500 内部同时完成交换和安全功能，如图 9-4 所示。

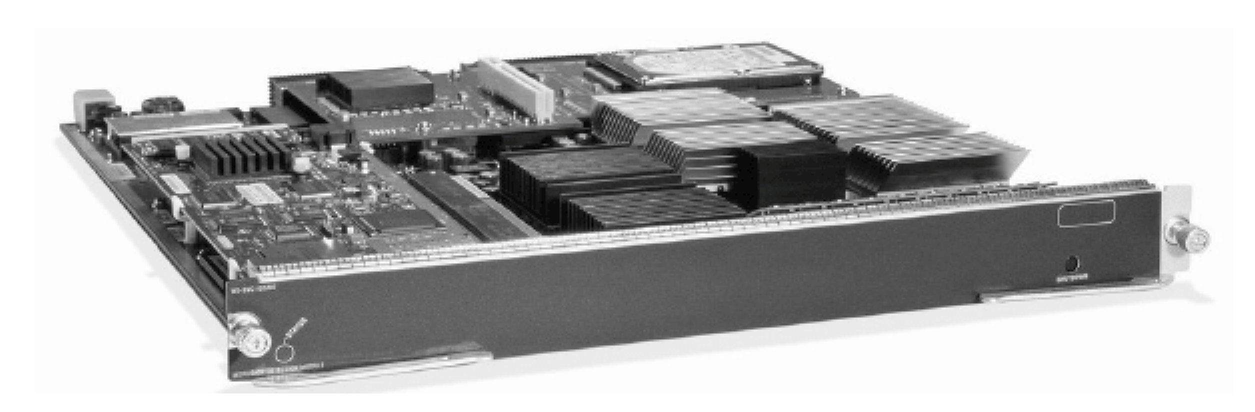


图 9-4 IDSM-2 模块

IDSM-2 模块除了可以和 IPS/IDS 4200 一样可以使用 SPAN(交换式端口分析器)、

RSPAN(远程交换式端口分析器)的方式进行流量捕获外，还可以支持 VACL 的方式进行流量捕获，同时它们使用的软件结构完全相同，其初始化方式也完全相同。

下面描述了 IPS/IDS 4200 和 IDSM-2 模块的初始化过程。

❶ 如果使用的是 IPS/IDS 4200，可以直接通过 Console 方式进行登录。如果使用的是 IDSM-2 模块，则需要从交换机的特殊模式下登录到该模块上。

```
Cat6500#session slot 6 processor 1
```

❷ 对 IPS/IDS 4200 和 IDSM-2 模块进行初始化配置，并重新启动。

```
sensor(config)# service host
sensor(config-hos-net)#network-settings
sensor(config-hos-net)#host-ip 192.168.1.200/24， 192.168.1.1
                            //配置管理接口IP地址和网关
sensor(config-hos-net)#host-name ips-sensor    //配置主机名
sensor(config-hos-net)#telnet-option enabled      //开启telnet选项
sensor(config-hos-net)#access-list 192.168.1.0/24    //配置管理地址网段
sensor(config-hos-net)#exit
sensor(config-hos)#time-zone-settings           //配置时区
sensor(config-hos-tim)#offset 8
sensor(config-hos-tim)#standard-time-zone-name beijing
sensor(config-hos-tim)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]:yes
Warning : Reboot is required before the configuration change will take effect
Warning : The node must be rebooted for the changes to go into effect.
Continue with reboot?[yes]:yes
```

❸ 为了方便管理，重新启动后在 IDSM-2 模块上配置 Web 服务，这样以后通过浏览器就可以配置该模块了。

```
sensor(config)# service web-server
sensor(config-web)# enable-tls true
sensor(config-web)# port 443
sensor(config-web)# exit
Apply Changes:?[yes]: yes
```

4. 监控流量导入 IPS/IDS

通常，IPS/IDS 使用 SPAN 的方式在核心交换机上对复制出的监控流量进行分析。对于远程交换机的流量，可以通过 RSPAN 的方式进行监控，其部署方式如图 9-5 所示。

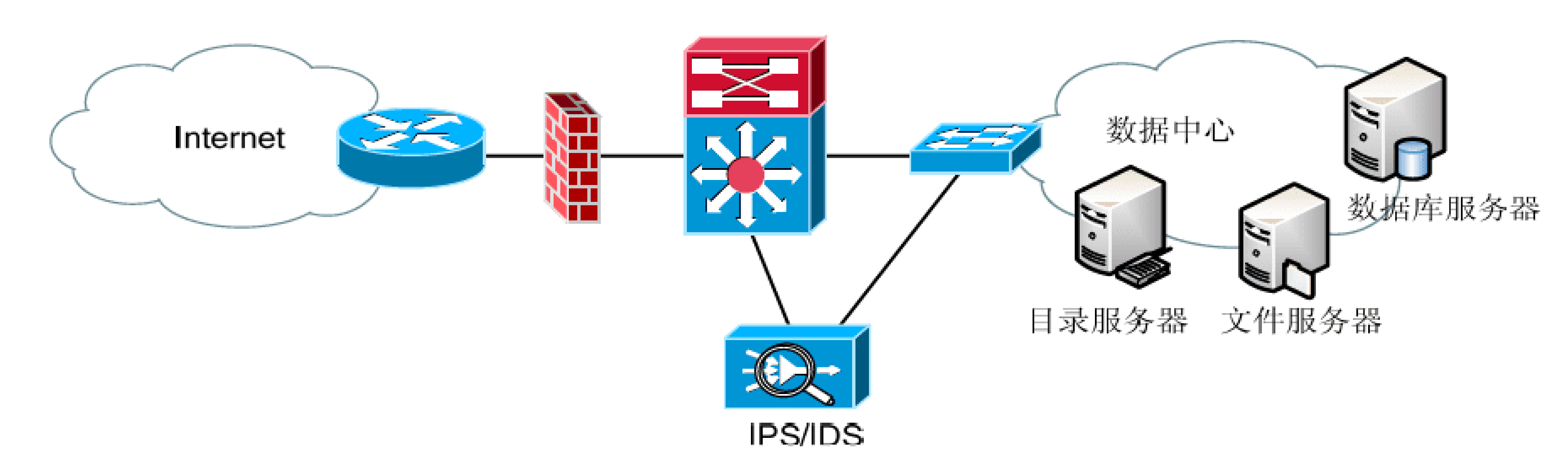


图 9-5　IPS/IDS 部署方式

❶ SPAN 可以监控多个 VLAN， Cisco 6500 系列交换机的配置的方式如下。

```
Cat6500(config)#no monitor session all
Cat6500(config)# monitor session 1 source vlan 10, 11, 100, 110
Cat6500(config)# monitor session 1 destination interface Fa1/1 encapsulation
dot1q
```

如果使用的交换机是 Cisco 3750，可按下述方法进行配置。

```
Cat3750(config)# monitor session 1 source vlan 10
Cat3750(config)#  monitor  session  1  destination  interface  Gi1/1/5
encapsulation replicate
```

❷ 若要对远程交换机进行流量控制，则需要配置 RSPAN。

在远程交换机做如下配置。

```
Cat3750(config)#vlan 500
Cat3750(config-vlan)#remote-span
Cat3750(config)# monitor session 1 source vlan 10
Cat3750(config)# monitor session 1 destination remote vlan 500
```

在本地交换机做如下配置。

```
Cat3750(config)#vlan 500
Cat3750(config-vlan)#remote-span
Cat3750(config)# monitor session 1 source remote vlan 500
Cat3750(config)# monitor session 1 destination interface fa0/12
```

❸ 在路由器上为 NM-CIDS 模块配置流量映射。

```
Router(config)# interface G0/0
Router(config-if)# ids-service-module monitoring
```

❹ ISDM-2 配置方式。ISDM-2 也支持 SPAN 和 RSPAN 的配置，配置方式和前述 IPS 4200 类似。

```
Cat3750(config)#vlan 500
Cat3750(config-vlan)#remote-span
Cat3750(config)# monitor session 1 source vlan 10
Cat3750(config)# monitor session 1 destination remote vlan 500
Cat6500(config)#no monitor session all
Cat6500(config)# monitor session 1 source remote vlan 500
Cat6500(config)# monitor session 1 destination intrusion-detection-module
6 data-port 1
```

ISDM-2 还支持基于 VLAN 的交换式端口分析器(VSPAN)，其配置方式如下。

```
intrusion-detection module 6 management-port access-vlan 200
intrusion-detection module 6 data-port 1 capture
intrusion-detection module 6 data-port 1 capture allowed-vlan 10-15, 100-105
!
vlan access-map isdmvacl 10
match ip address 100
action forward capture
vlan access-map isdmvacl 20
match ip address 101
action forward
!
vlan filter isdmvacl vlan-list 10-15, 100-105
```

```
!
access-list 100 permit tcp any 192.168.1.0 0.0.0.255
access-list 101 permit ip any any
```

❺ ASA AIP-SSM 可以通过“https://<ASA-ip-address>ASDM”上的软件进行配置。

5. 使用 IDM 配置 NM-CIDS

Cisco IDM(IDS 设备管理器)是一个基于 Web 的传感器配置和管理工具，它能通过 Internet Explorer、Netscape 或 Mozilla 等浏览器来访问和配置 NM-CIDS，默认情况下使用 SSL 连接以保证通信的安全。IDM 为基于 Java 的运行平台，并且需要控制台系统为 Java 分配 256MB 内存。

下面简要地介绍一下通过 IDM 来配置和管理 NM-CIDS 的操作过程。

❶ 在实施 NM-CIDS 管理的主机上，进入控制面板双击 Java 图标，如图 9-6 所示。



图 9-6　配置 Java

❷ 在【Java 控制面板】对话框中，选择 Java 选项卡，单击【设置】按钮，在【JavaRuntime 设置】对话框中添加“–Xmx256m”，将 Java Runtime 所使用的内存调整为 256MB，如图 9-7 所示。



图 9-7　配置 Java Runtime 内存

❸ 在浏览器的地址栏中输入“https://< NM-CIDS”的 IP 地址以访问 NM-CIDS，这时会提示输入用户名和密码，如图 9-8 所示。



图 9-8　访问 IDM

❹ 输入用户名和密码后，便打开 IDM 控制台界面，如图 9-9 所示。

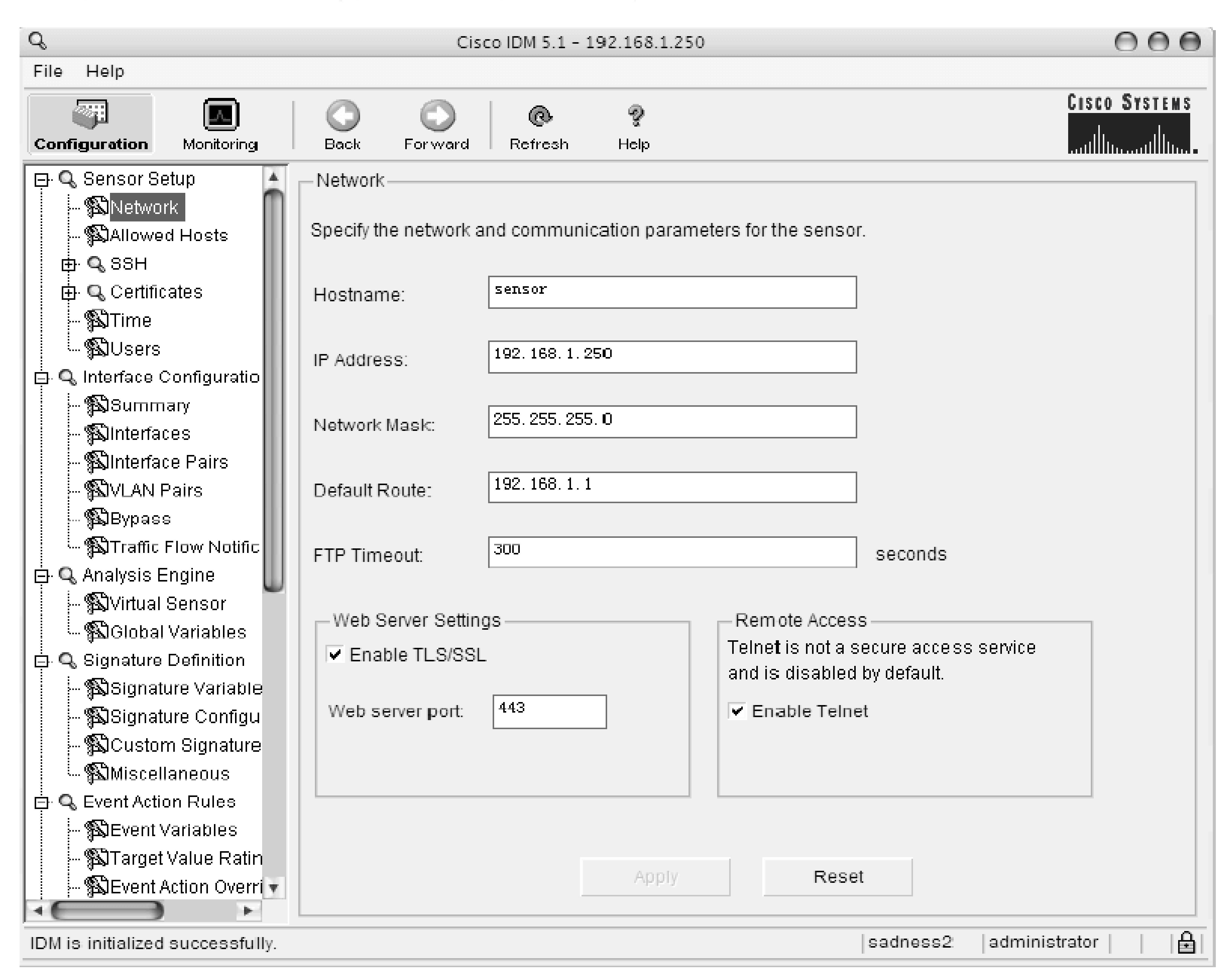


图 9-9　IDM 控制台界面

❺ 选择 Licensing 结点， 配置 IPS 进行授权信息升级。信息升级可以为用户提供动态的特征升级服务，保障 IPS 系统的安全性，如果用户没有签订 IPS 特征升级服务，可以在 Cisco 网站利用 IPS 主机序列号申请 60 天的试用授权。这种试用版授权只能申请一次，为了保证 IPS 持久更新，建议购买 IPS 信息库升级授权。升级时，可以选择使用 Cisco 网站进行在线升级，或者通过网上申请后，Cisco 会将授权文件发往申请人的邮箱中，通过文件本地授权，

如图 9-10 所示。

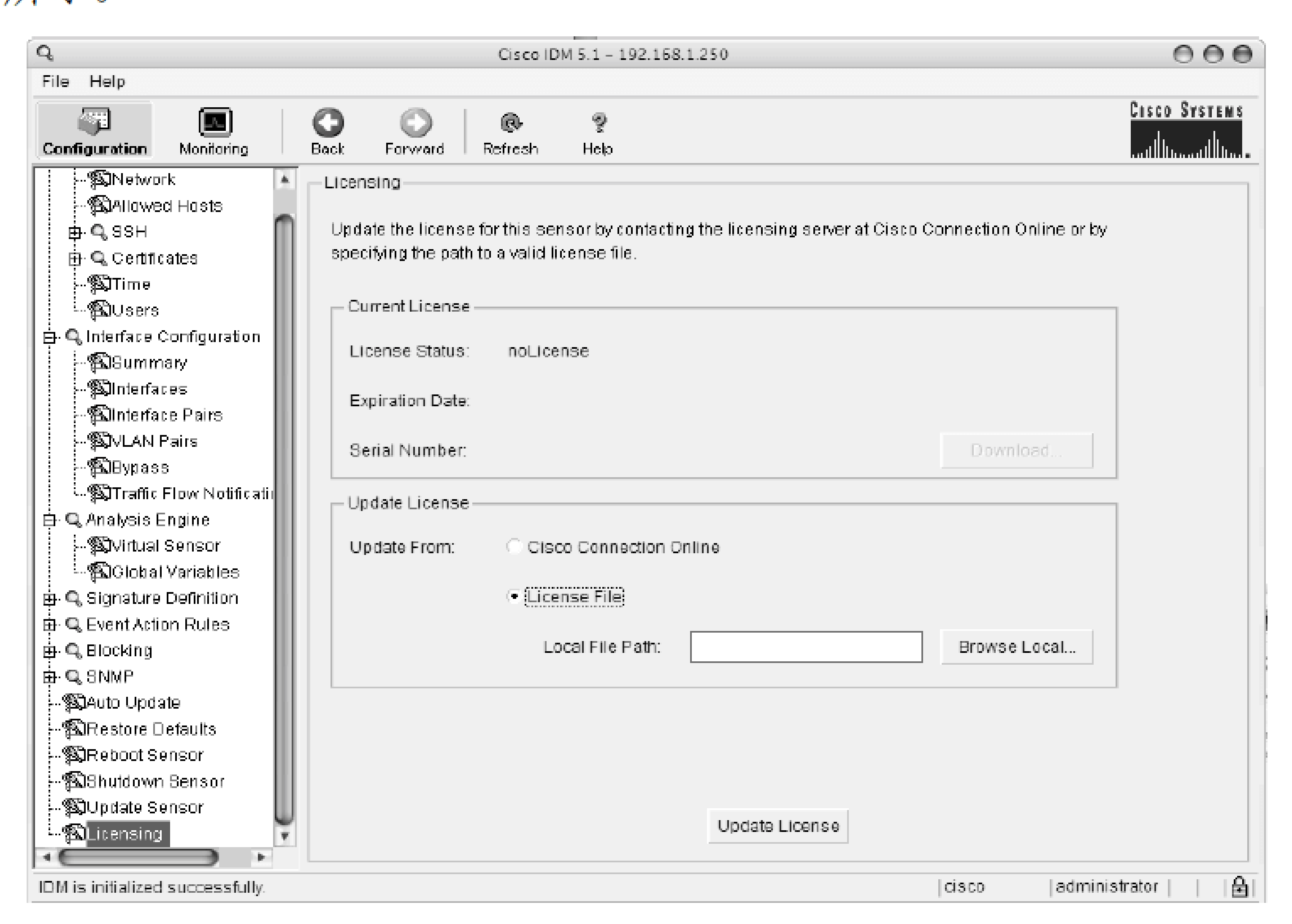


图 9-10　配置 license

❻ 完成授权后，才可以升级 IPS 特征库。特征库可以通过在 Cisco 官方网站下载后，通过 IDM 选择 Update Sensor 进行本地升级，如图 9-11 所示。

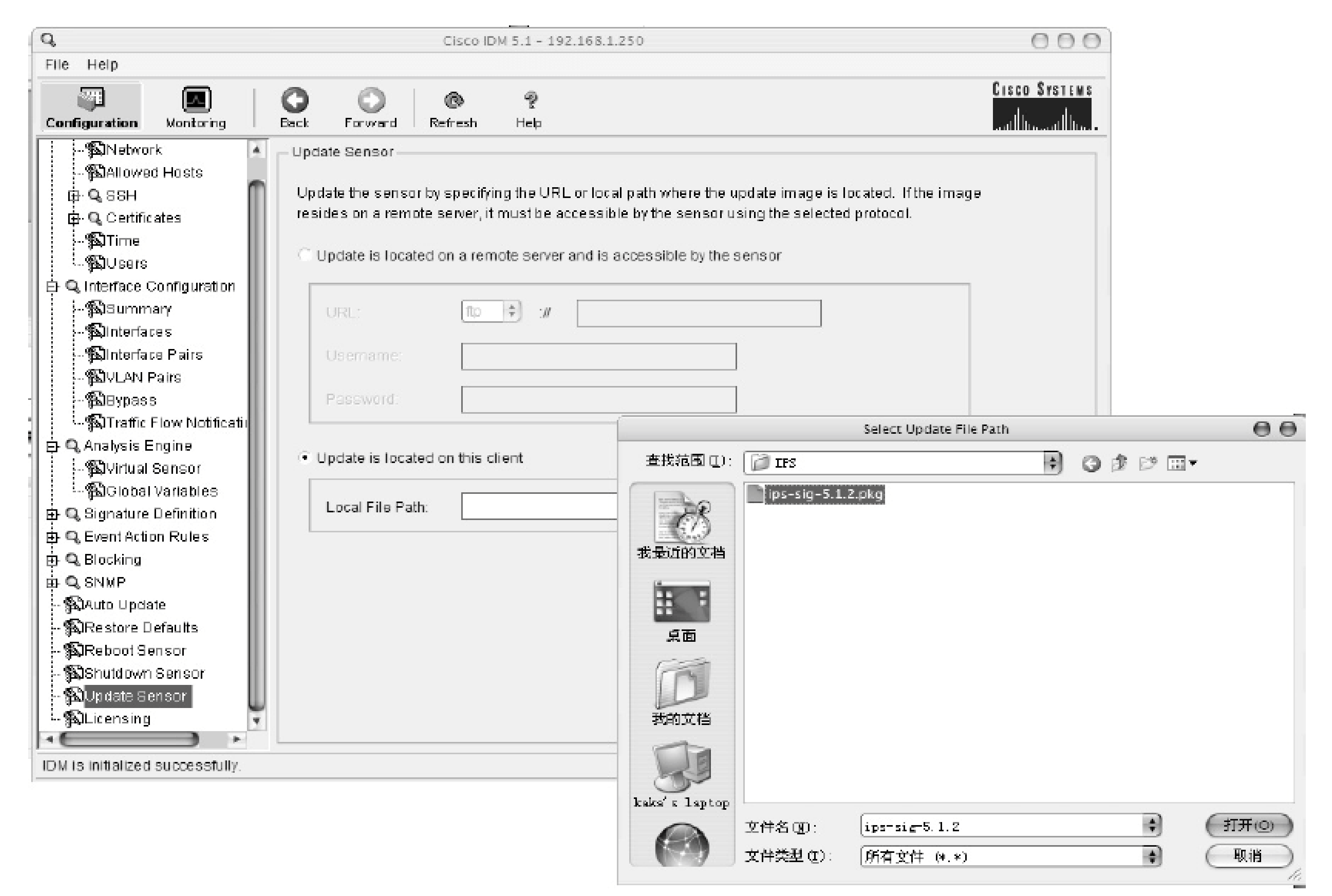


图 9-11　升级特征库

❼ 依次选择 Interface Configuration→ Interfaces 结点，并选择相应的接口，单击 Enabled 按钮开启流量采集功能，如图 9-12 所示。

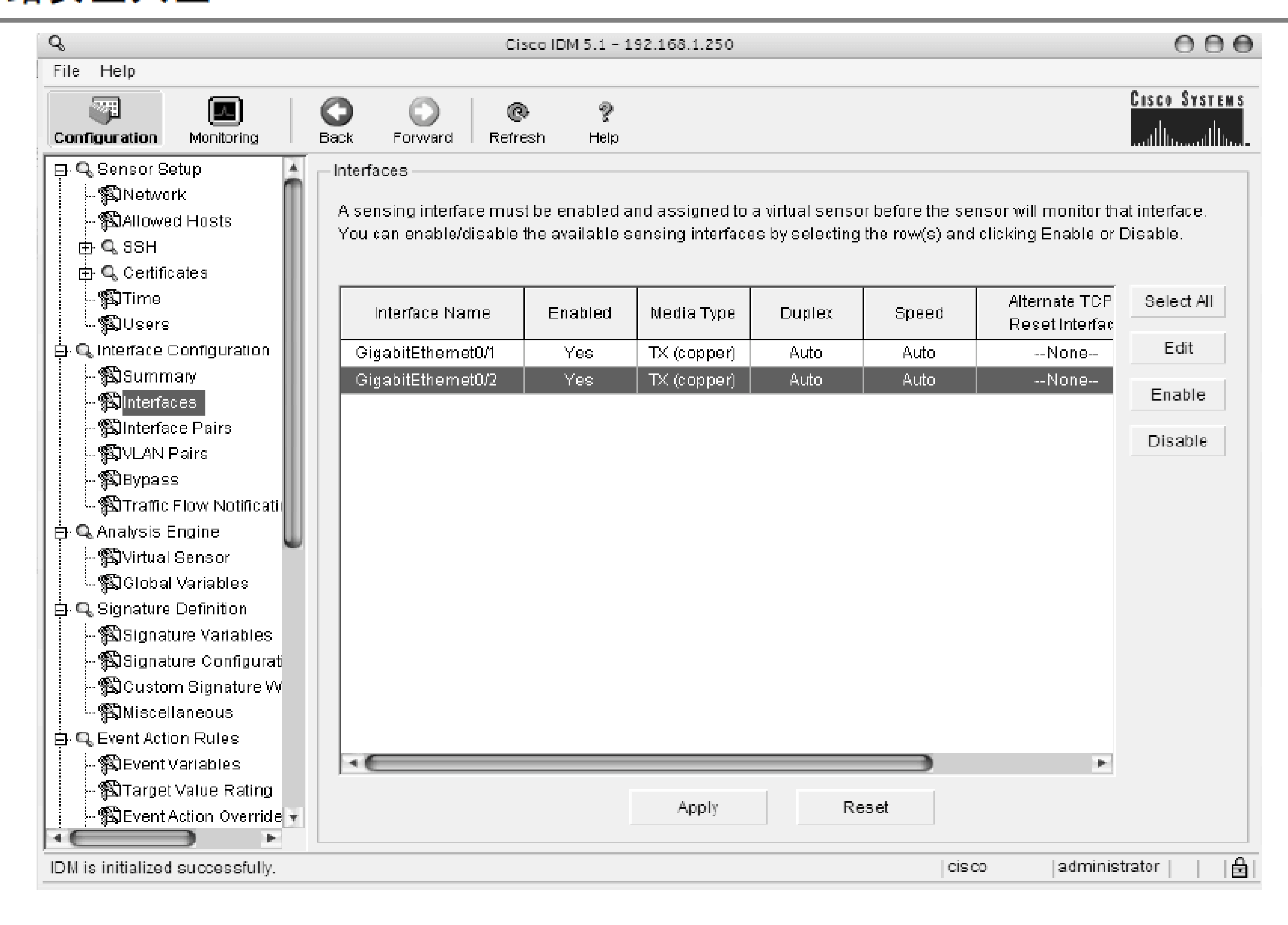


图 9-12 开启流量采集功能

❽ 依次选择 Analysis Engine→Virtual Sensor 结点，将所使用的监控端口加入到 vs 中，如图 9-13 所示。

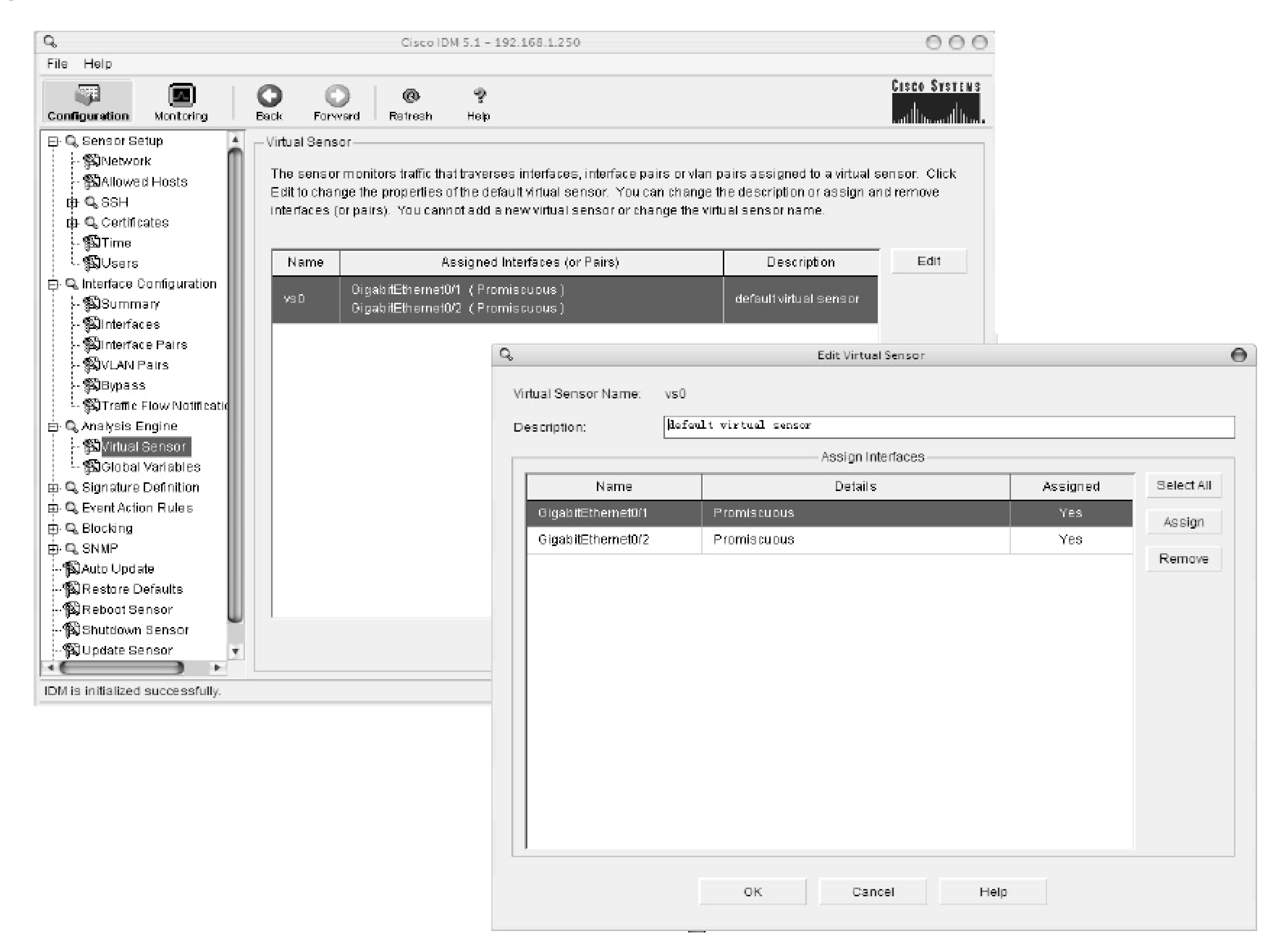


图 9-13 将端口加入到 Virtual Sensor 中

❾ IPS/IDS 可以与 PIX/ASA/FWSM 通过 SHUN 进行联动，与 Catalyst 6500 通过 VACL 进行联动，与 ISR 路由器通过 ACL 进行联动。依次选择 Blocking→ Device Login Profiles 结点，

为 IPS 配置联动设备的登录用户名，如图 9-14 所示。

图 9-14　配置 Login Profile

⑩ 依次选择 Blocking→ Blocking Devices 结点，配置相应的设备，并关联上一步配置的登录策略，如图 9-15 所示。

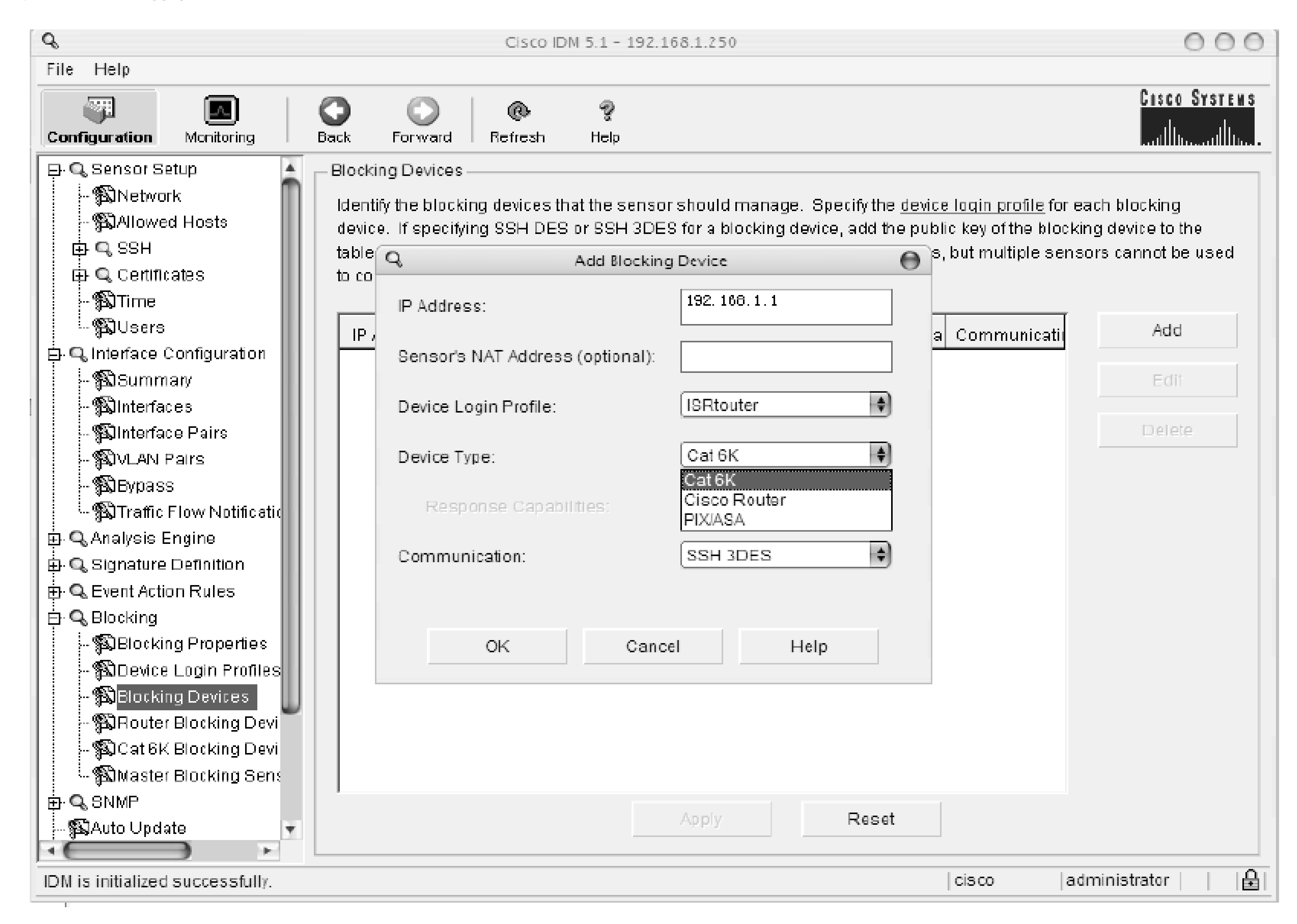


图 9-15　配置联动设备

⑪ 在 Router Blocking Device Interface 和 Cat 6K Blocking Device Interface 结点中，还可以通过 VACL、ACL 进行配置，如图 9-16 所示。

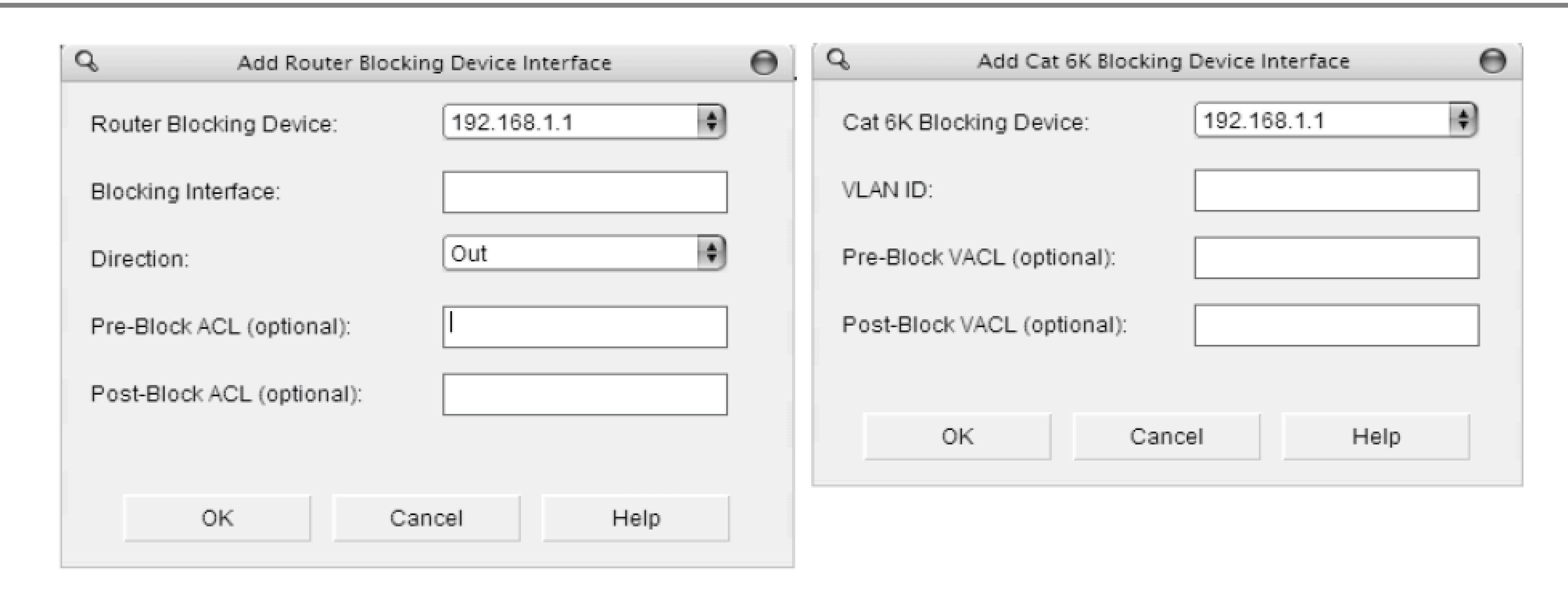


图 9-16　配置 ACL、VACL

⓬ 我们可以使用两种方式配置 IPS 与网络设备联动时所执行的策略。一种是单独调节特征码的执行策略，避免一些特征码误报而产生的不必要的拦截。依次选择 Signature Definition→Signature Configuration 结点，并在右侧窗格选择相应的 Signature，单击 Disable 按钮关闭，或者双击配置事件的行为，如图 9-17 所示。

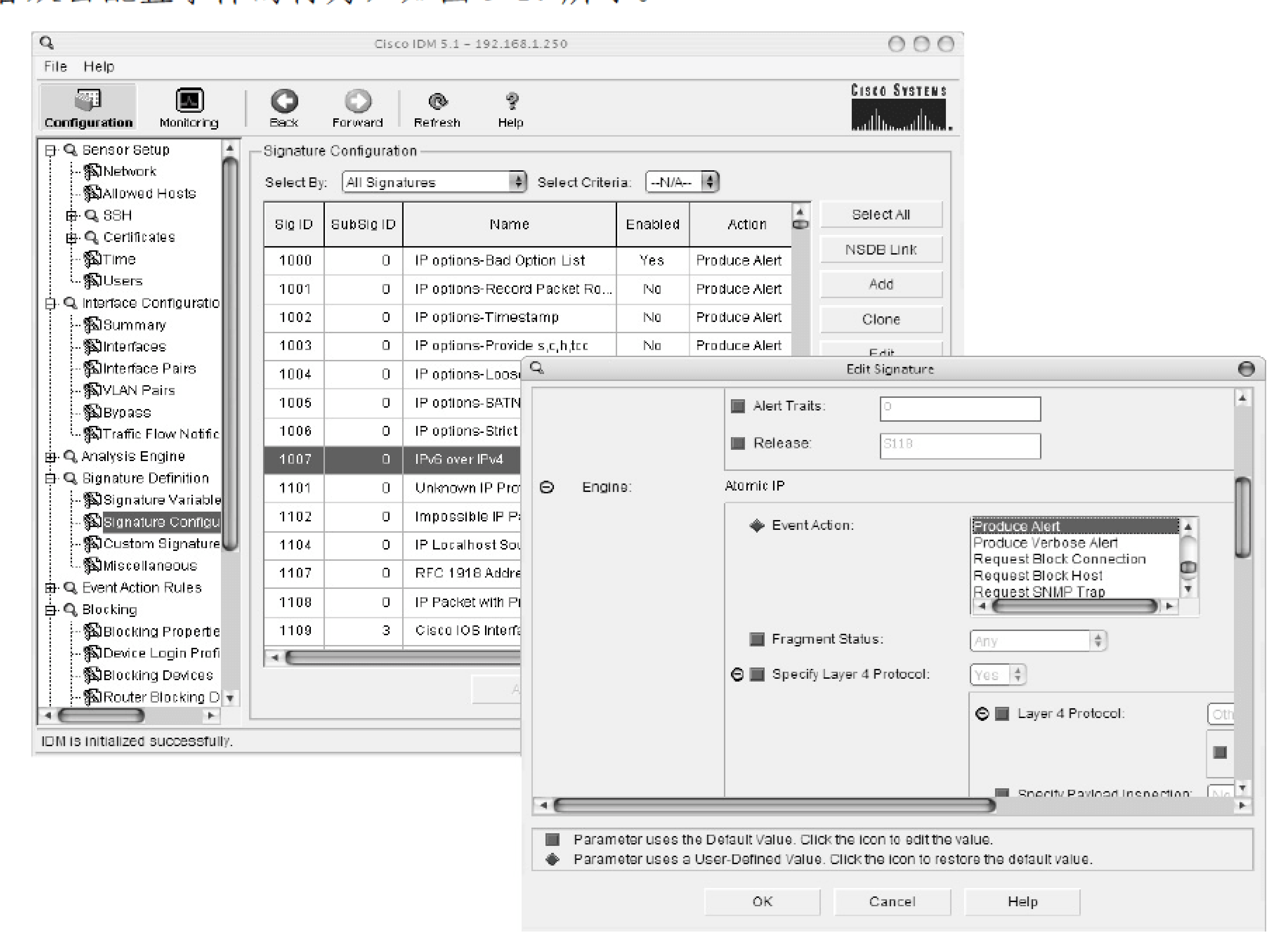


图 9-17　自定义特征码

⓭ 依次选择 Event Action Rules →Event Action Overrides 结点，调节 Rise Rating 进行联动配置并且这样的方式可以统一执行策略，避免单独调整特征库的行为，如图 9-18 所示。

⓮ 依次选择 Event Action Rules →General Settings 结点，设置被拦截后禁止访问的时间，如图 9-19 所示。

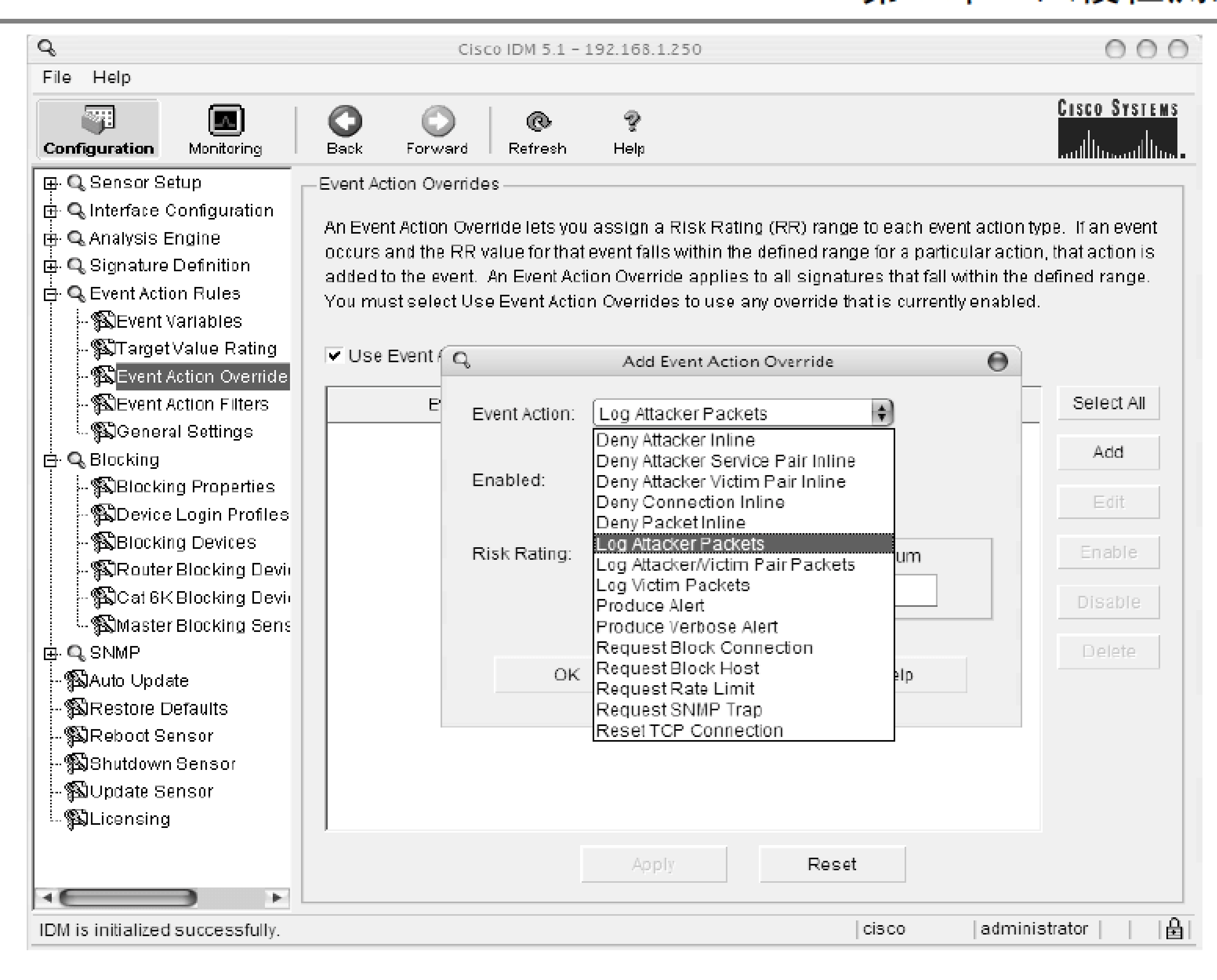


图 9-18　配置事件响应行为

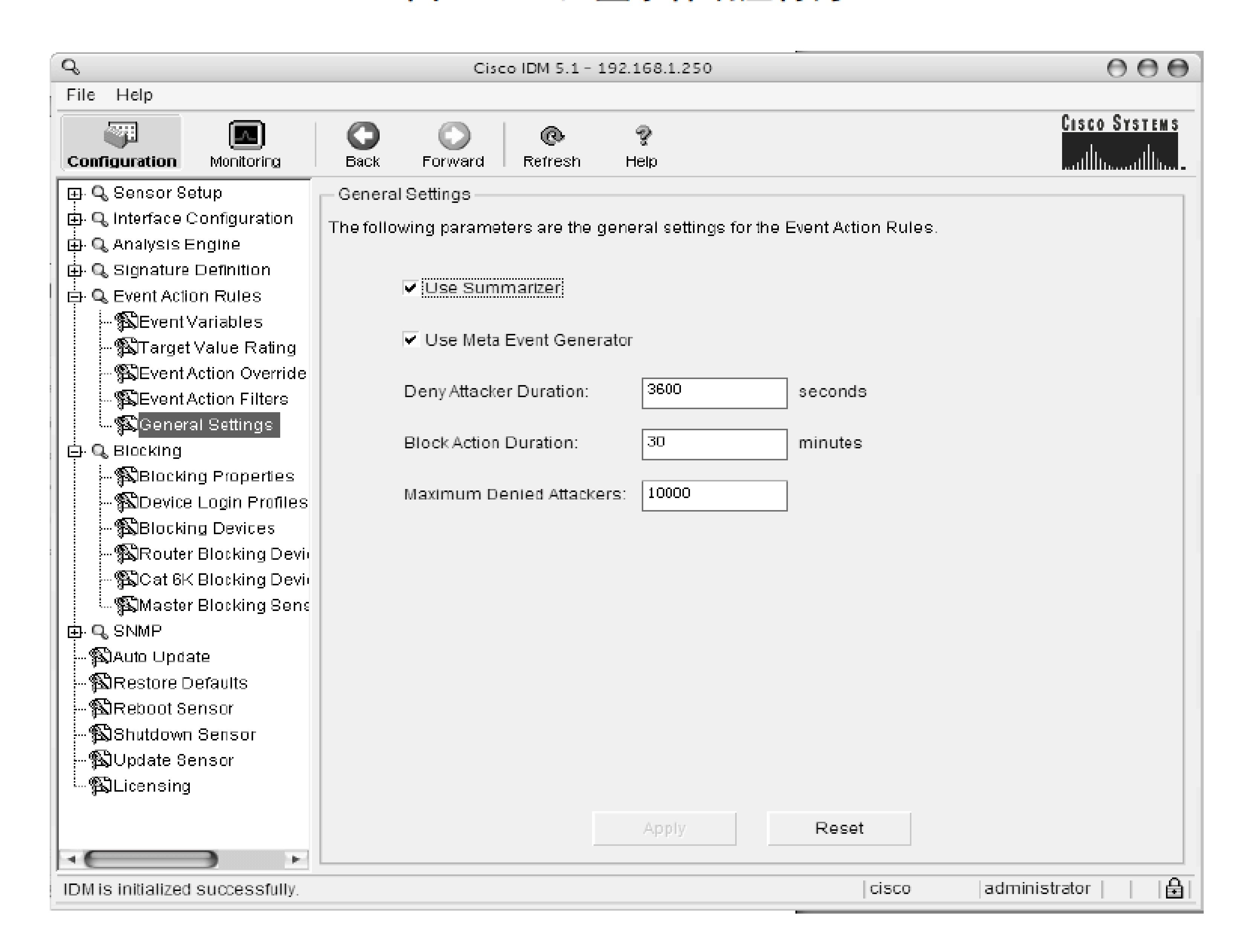


图 9-19　配置拦截后的禁止询问的时间

15 对于一些关键业务段，例如订单处理系统等，我们为了防止误报或者一些其他行为导致业务中断，需要将这些网段排除在监控范围外。配置方法是依次选择 Blocking→Blocking Properties 结点，添加 Never Block Address 属性，如图 9-20 所示。

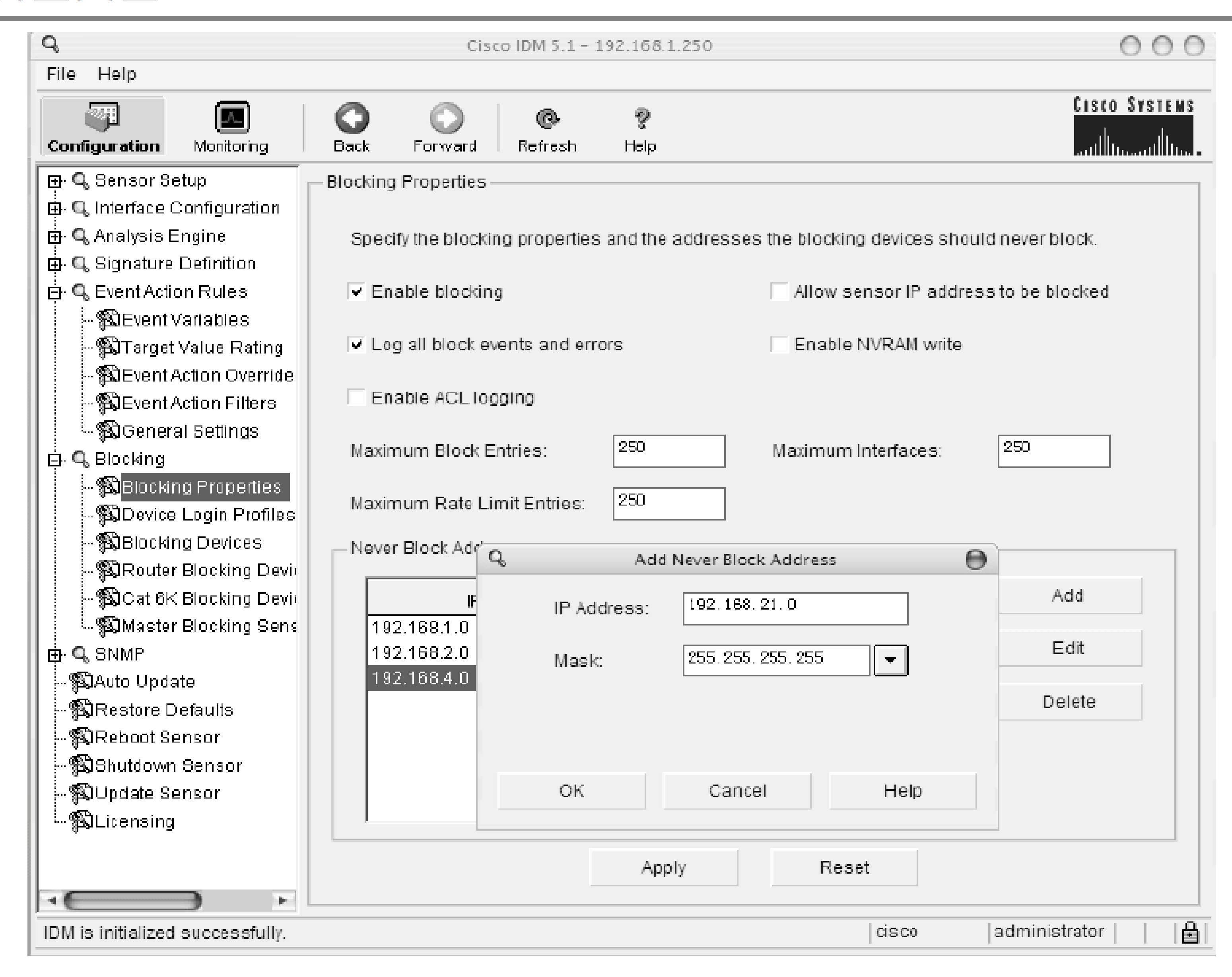


图 9-20 添加不进行监控的地址段

6. 配置 IPS/IDS 工作模式

在第 8 章已经介绍了 AIP-SSM 模块可以配置为旁挂模式和串行模式。同样 IPS 4200 和 ISDM-2 也可以配置为串行模式。

在传统的旁挂模式中，IPS 通过监测由交换机复制到监控口的流量，进行入侵分析，并通过 Shun 消息、ACL、VACL 控制网络设备，如图 9-21(a)所示。但是，旁挂模式也有一些缺陷，例如网络中的很多非 Cisco 的设备将无法识别入侵防御产生的控制消息，使得入侵防御失效，因此我们需要将 IPS 配置为串行模式，如图 9-21(b)所示。

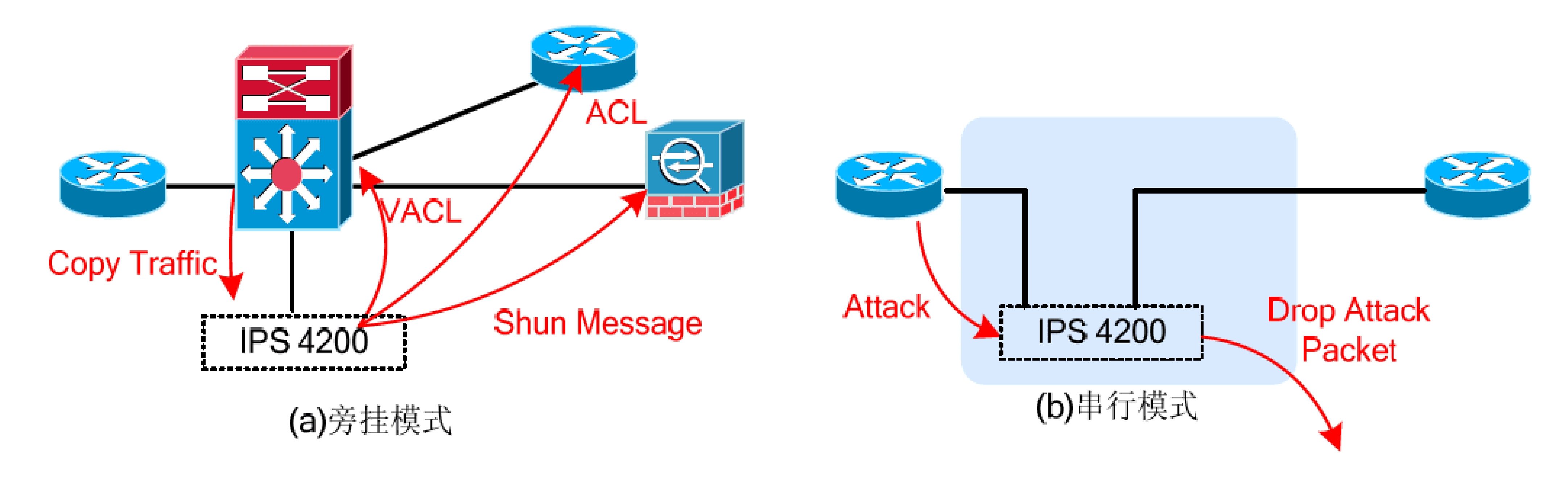


图 9-21 IPS 4200 接入模式

❶ 在 IDM 控制台界面中，选择 Interface Configuration→Interfaces 结点，并选择相应的接口，然后单击 Enabled 按钮开启流量采集功能，如图 9-22 所示。

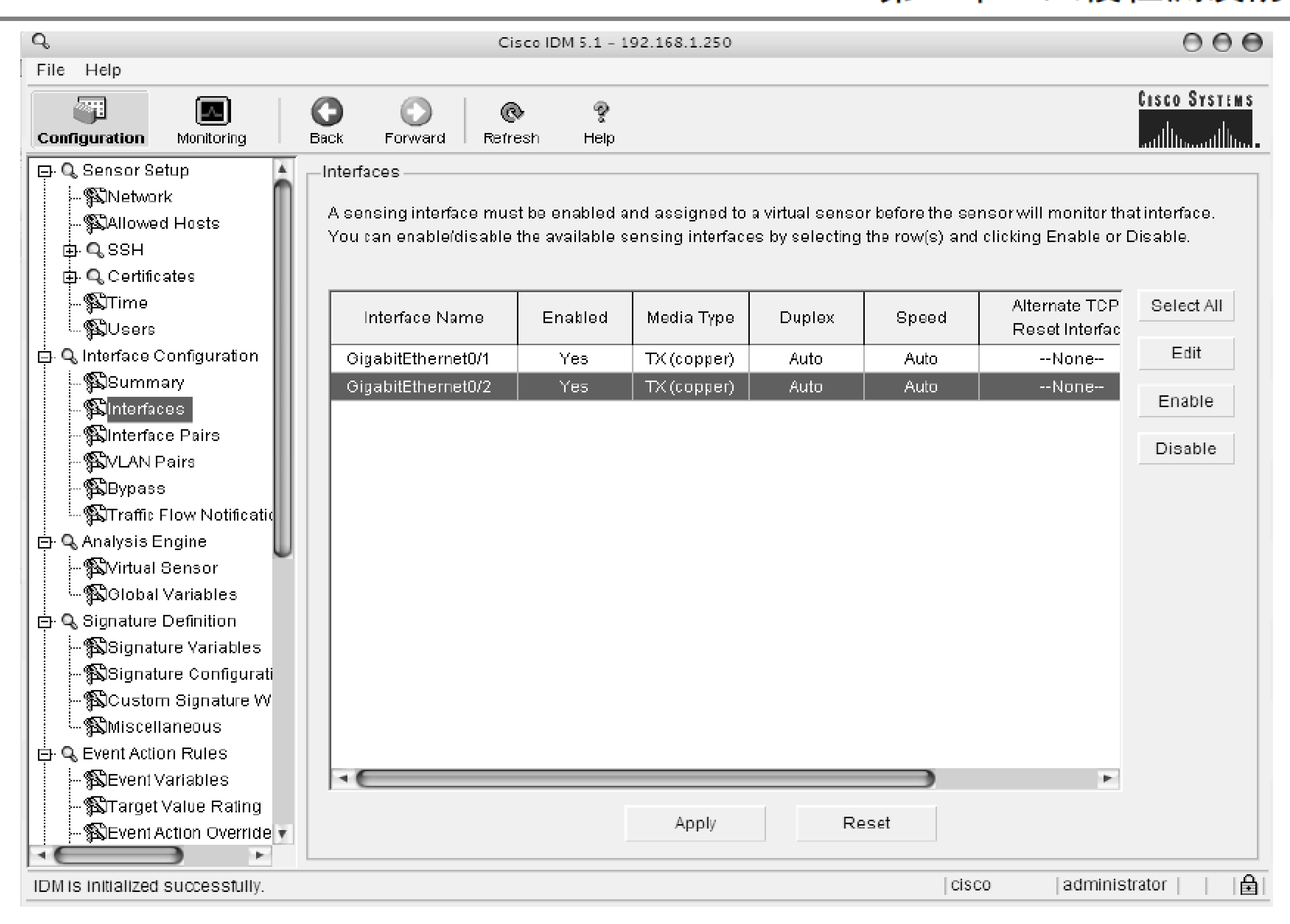


图 9-22　开启流量采集功能

❷ 选择 Interface Configuration→Interfaces Pairs 结点，配置接口对，如图 9-23 所示。

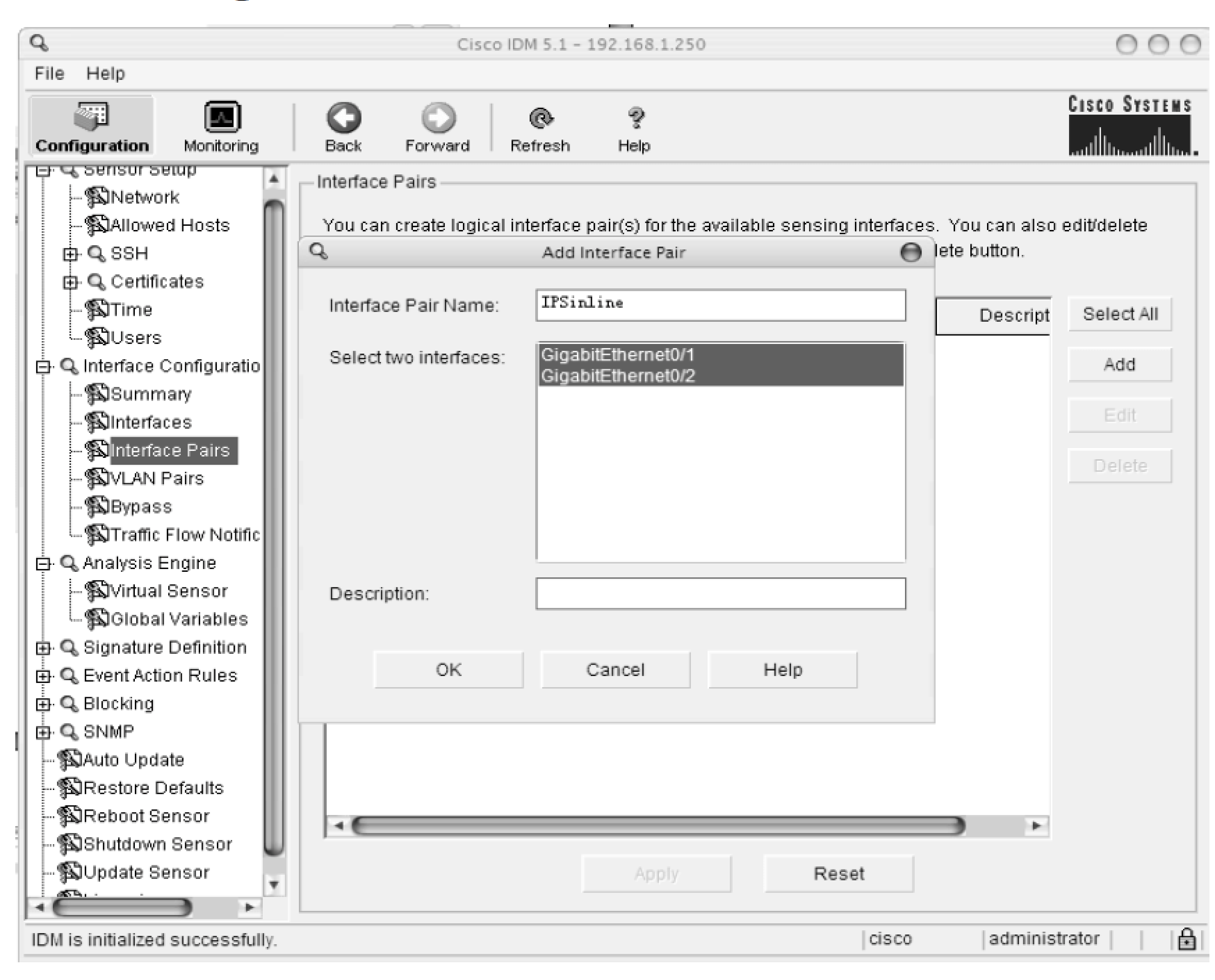


图 9-23　配置接口对

对于交换机内置的 ISDM-2 模块，也可以配置 Vlan Pairs，如图 9-24 所示。

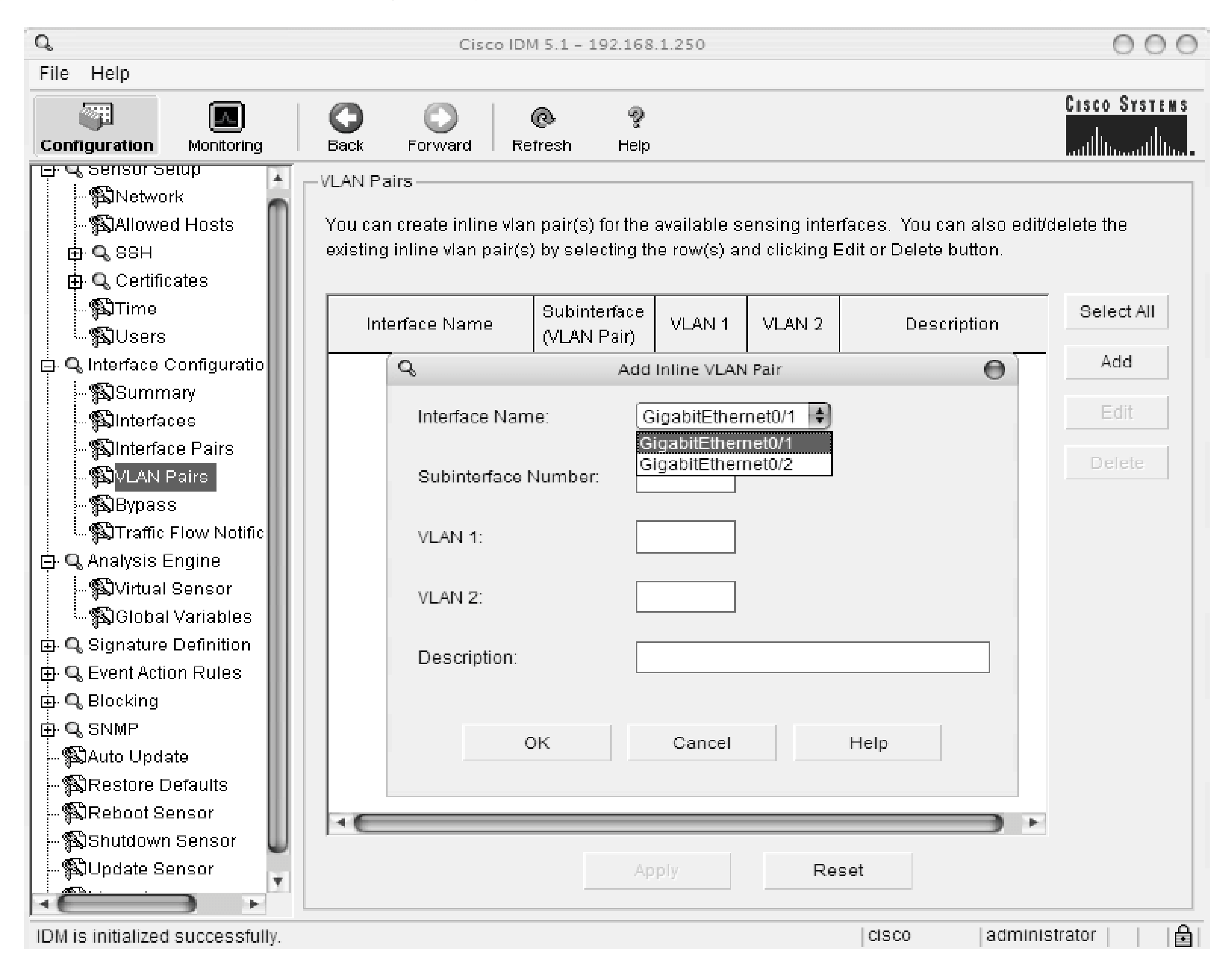


图 9-24　配置 VLAN 对

❸ 选择 Analysis Engine→ Virtual Sensor 结点，将所使用的监控接口对加入到 vs 中，如图 9-25 所示。

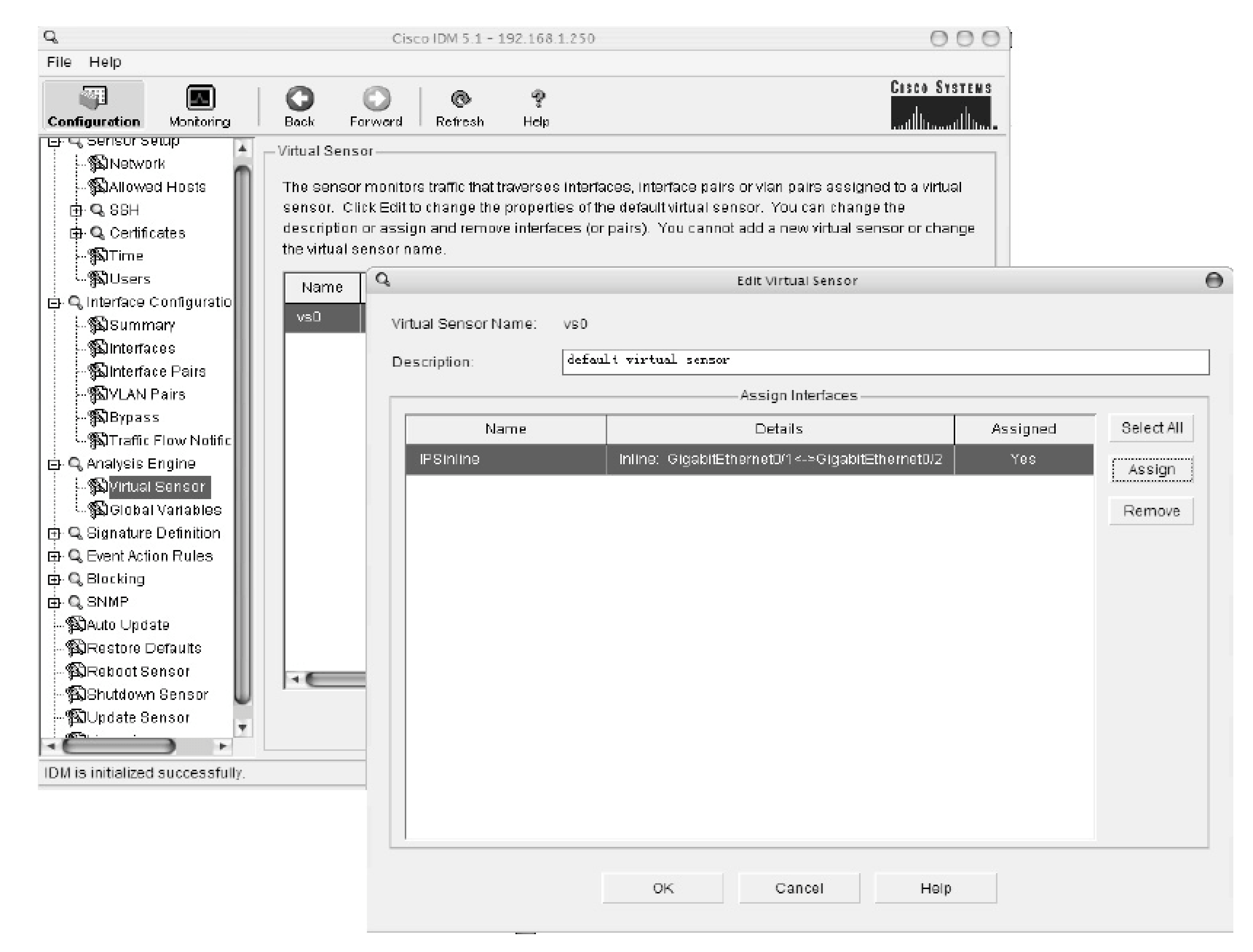


图 9-25　分配接口到 Virtual Sensor

❹ 选择 Signature Definition→ Signature Configuration 结点，在右侧窗格中选择相应的特征码配置串行策略。当一个特征码检测到攻击，在串行模式下 Enter Action 可设置为 Deny Attacker Inline、Deny Connection Inline、Deny Packet Inline 等 3 种操作，对包进行丢弃，如图 9-26 所示。

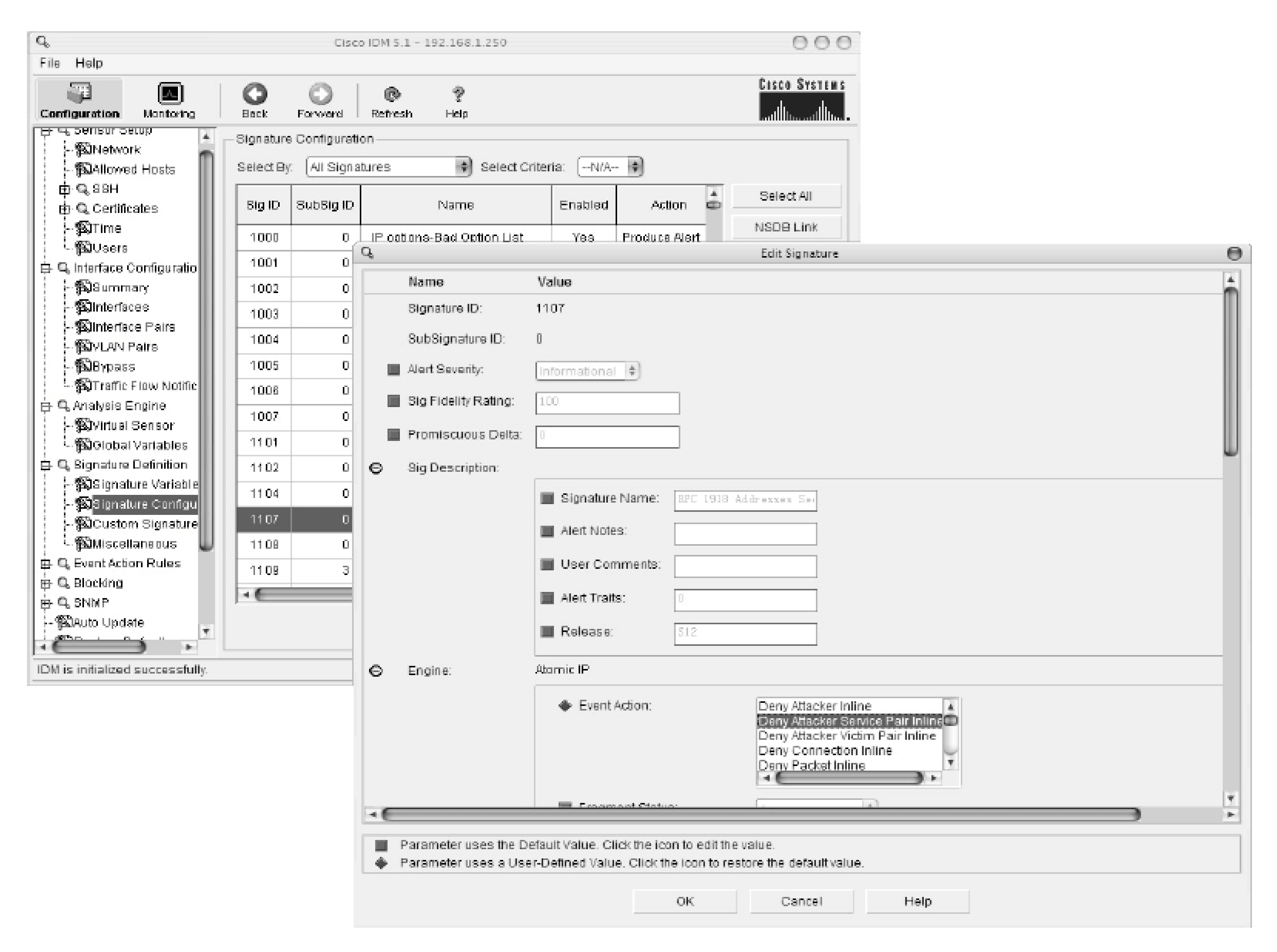


图 9-26　配置特征码

❺ 选择 Interface Configuration→ Bypass 结点，打开 Bypass 功能，用于 IPS 发生故障时不影响业务数据流，如图 9-27 所示。

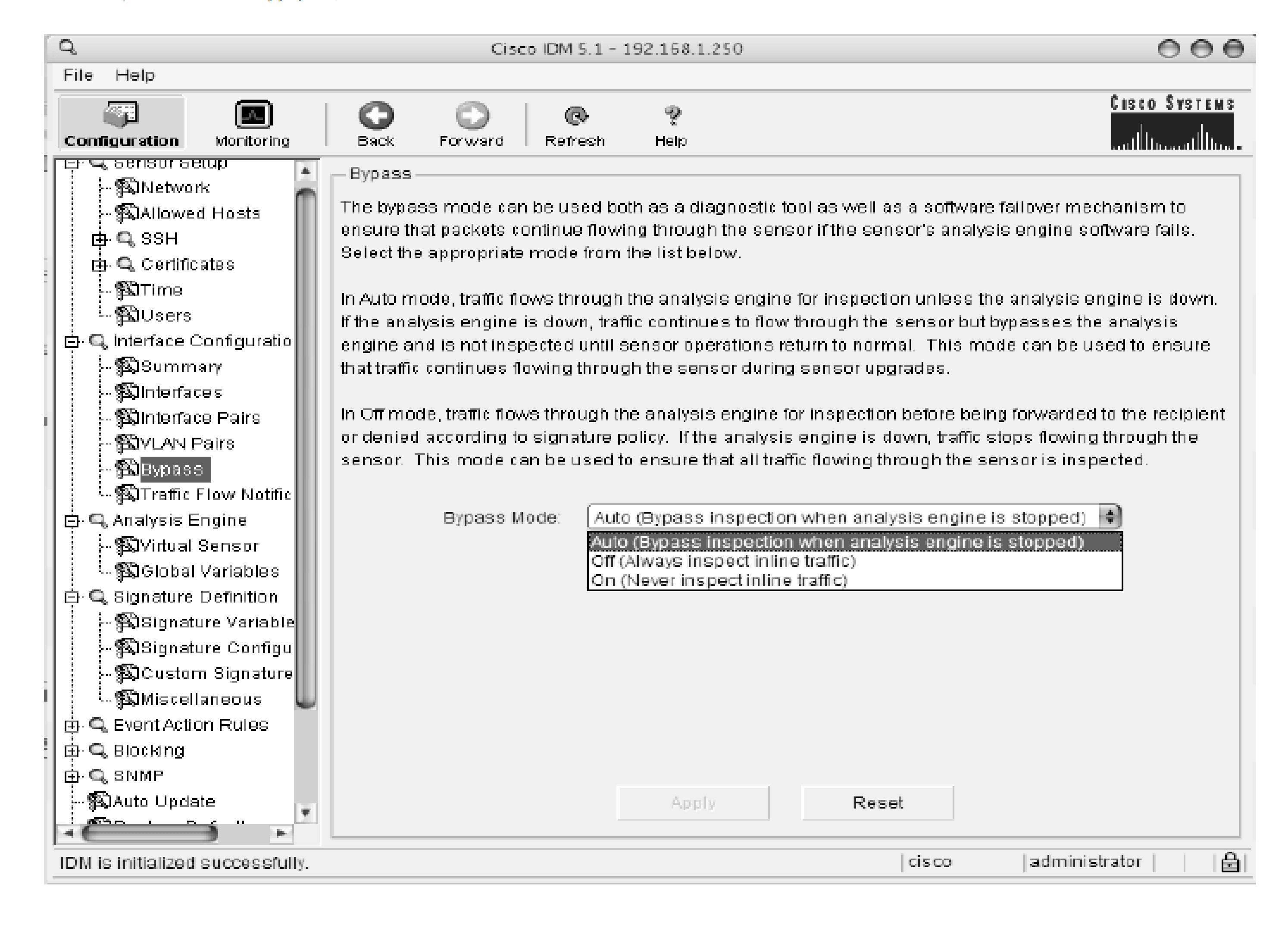


图 9-27　配置 Bypass

9.3 Snort

Snort 是一个轻便的网络入侵检测系统，可以完成实时流量分析和对网络上的 IP 包登录进行测试等功能，能完成协议分析、内容查找 / 匹配，能用来探测多种攻击和嗅探(如缓冲区溢出、秘密断口扫描、CGI 攻击、SMB 嗅探、指纹采集尝试等)。

Snort 有 3 种工作模式：嗅探器、数据包记录器和网络入侵检测。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上；数据包记录器模式把数据包记录到硬盘上；网路入侵检测模式是最复杂的，而且是可配置的，用户可以让 Snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的行动。

Snort 通常与 ACID(Analysis Console for Intrusion Databases，入侵数据库分析控制台)配合，在基于 Apache+Mysql+PHP 的 Linux 平台上进行部署，下面简要地介绍一下其配置过程。

❶ 按照下述步骤安装 Snort。

```
# tar zxvf snort-2.3.3.tar.gz
# tar zxvf snort-2.0.0.tar.gz
# cd snort-2.3.3
# ./configure --with-mysql=/usr/local/mysql
# make
# make install
# cd rules
# mkdir /etc/snort
# mkdir /var/log/snort
# cp * /etc/snort
# cd ../etc
# cp snort.conf /etc/snort
# cp *.config /etc/snort
```

❷ 需要在 mysql 中为 Snort 创建数据库。

```
 /usr/local/mysql/bin/mysql -uroot -pcisco123
# create database snort;
# grant INSERT, SELECT on root.* to snort@localhost;
# exit
```

❸ 配置 Snort 的配置文件 Snort.conf。

```
Var HOME_NET 192.168.0.0/24
//修改var HOME_NET 为需要监控的LAN地址段
output database: log, mysql, user=root password=sadness123 dbname=snort
host=localhost
//配置输出到mysql数据库，并指定数据库用户名、密码和表名
var RULE_PATH /etc/snort
//指定规则库的路径
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/shellcode.rules
include $RULE_PATH/policy.rules
include $RULE_PATH/porn.rules
include $RULE_PATH/info.rules
include $RULE_PATH/icmp-info.rules
```

```
include $RULE_PATH/virus.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/p2p.rules
//引用相关的规则库，如果不需要某库，可以通过#去掉
```

4 按照下述步骤安装 ACID。

```
cp acid-0.0.6b23.tar.gz /www/htdocs
cd /www/htdocs
tar -xvzf acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz
```

5 配置 ACID 的配置文件 acid_conf.php。

```
cd /www/htodcs/acid/
vi acid_conf.php
//按照如下方式进行修改
$DBlib_path = "/usr/local/apache/htdocs/adodb"
$ChartLib_path = "/usr/local/apache/htdocs/jpgraph/src
  $alert_dbname   = "snort";
  $alert_host     = "localhost";
  $alert_port     = "";
  $alert_user     = "root";
  $alert_password = "cisco123";  //mysql密码

  /* Archive DB connection parameters */
  $archive_dbname   = "snort";
  $archive_host     = "localhost";
  $archive_port     = "";
  $archive_user     = "root";
  $archive_password = "cisco123"; //mysql密码
```

6 按照如下方式为 Snort 创建启动脚本。

```
# cd /usr/local/
# vi snort.sh
//添加:
#!/bin/sh
snort -d -h 192.168.0.0/24 -l /var/log/snort -c /etc/snort/snort.conf -i
 eth0 -A full
//完成后关闭该文件，并配置执行权限:
# chmod 755 snort.sh
```

7 启动相关服务后，通过登录地址 “http://<linux-ids-ipaddress>/acid/acid_main.php”，依次单击 Setup Page→Create ACID AG 链接，创建一个 ACID AG，如图 9-28 所示。

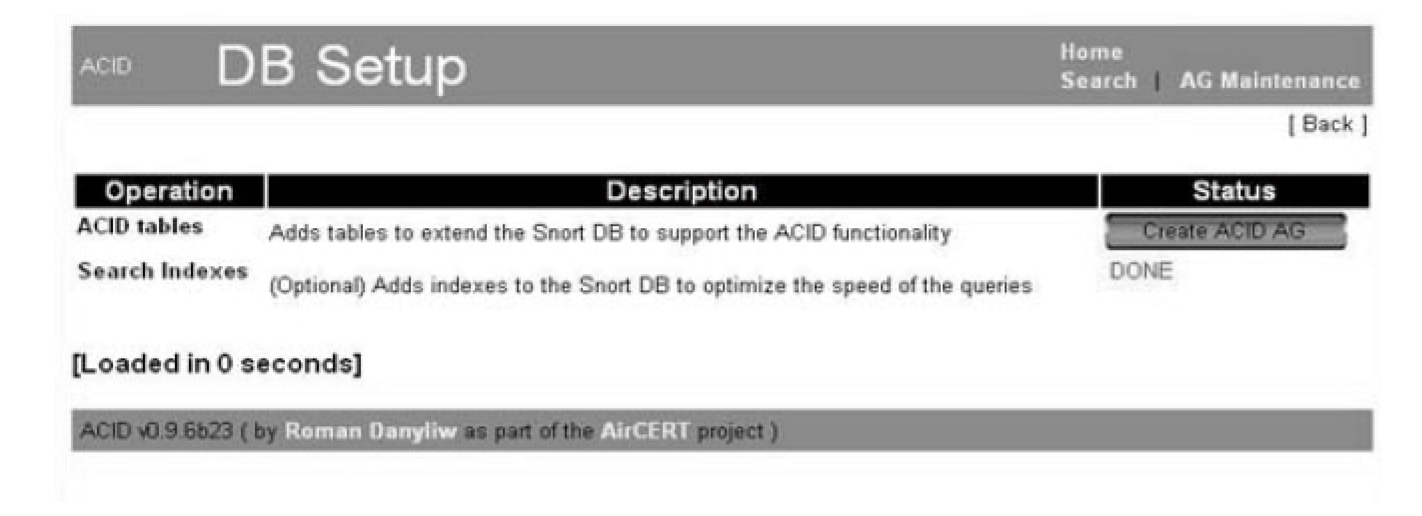


图 9-28　创建 ACID AG

❽ 配置完成后，用户可以通过 ACID 查看到 Snort 日志，如图 9-29 所示。

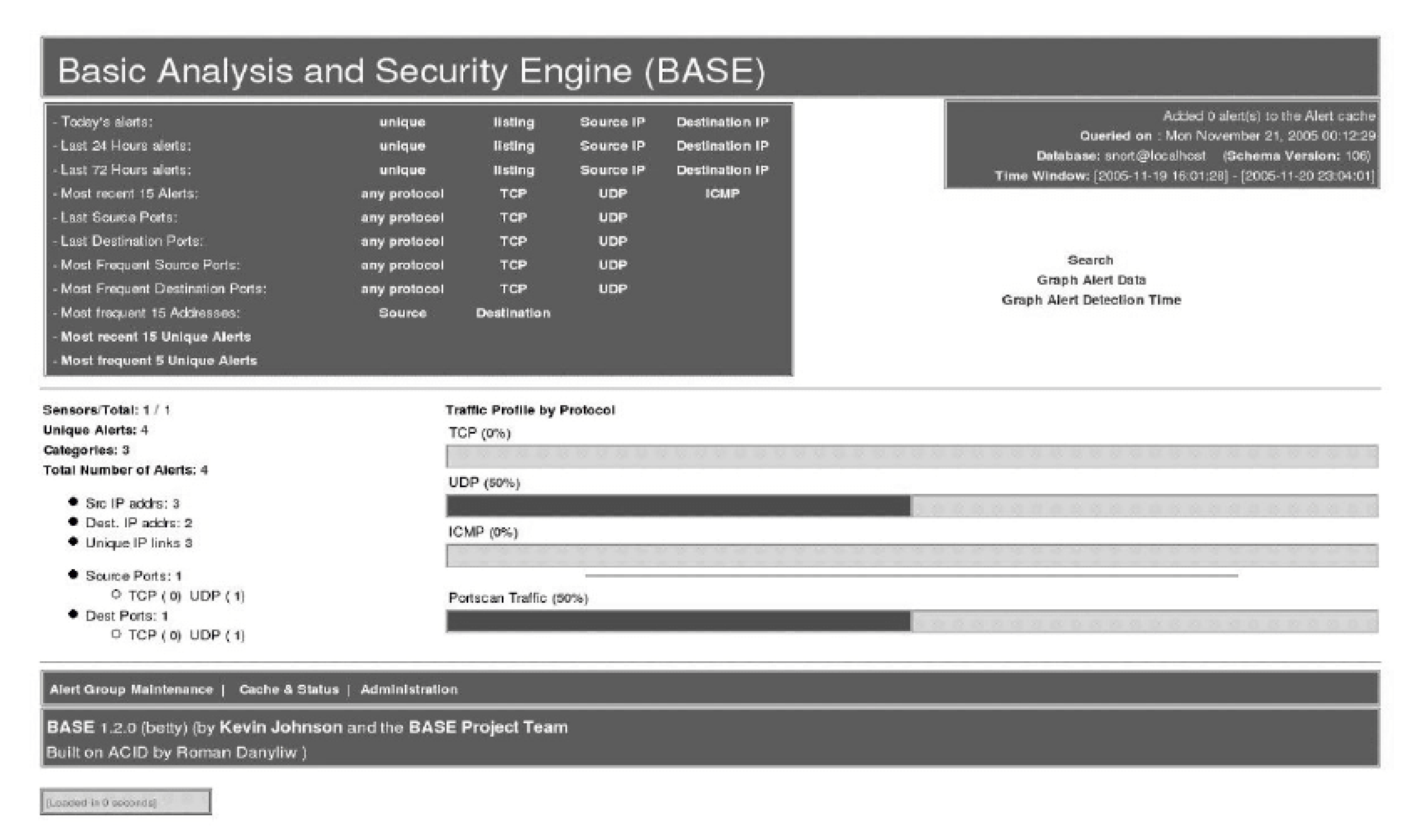


图 9-29　查看 Snort 日志

9.4　DDoS 检测与防御

1988 年 11 月 2 日，一个名叫 Robert Morris Jr.的大学生写了一个逻辑炸弹——蠕虫程序入侵 Internet。这个蠕虫程序在 Internet 上快速传播，当时造成整个网络中 15%(大约 6000 个)的系统都受到感染并停止运行。这就是第一次的 DoS 攻击。

从 20 世纪 90 年代到现在，DoS 技术主要经历的阶段如下所述。

- ✧ 技术发展时期。90 年代，Internet 开始普及，很多新的 DoS 技术涌现。90 年代末发明和研究过许多新的技术，其中大多数技术至今仍然有效，且应用频度相当高。著名的 DoS 攻击方式如 Ping of death、smurf、SYN flooding 等。
- ✧ 从实验室向“产业化”转换。2000 年前后，DDoS 出现，Yahoo、Amazon 等多个著名网站受到攻击并瘫痪。另外还有 Codered、SQL slammer 等蠕虫造成的事件。
- ✧ “商业时代”。最近一两年，宽带的发展使得接入带宽增加，个人电脑性能大幅提高，使 DDoS 攻击越来越频繁，可以说随处可见，而且也出现了更专业的出租“Botnet”(僵尸网络)的“DDoS 攻击经济”。可以说 DDoS 攻击的威胁已经无处不在，而且这样的攻击已经出现逐渐转化成一种新型犯罪行为的趋势。

9.4.1　DDoS 攻击原理

DDoS 攻击通过大量的数据流量使得网络设备和服务器不堪重负，或者构造特殊的报文使得服务器发出大量的响应而耗光资源。这样的做法具有明显的目的性，使得被攻击方服务瘫痪，从而导致其受到巨大的商业损失，同时还伴随着巨大的信誉损失。

在 2002 年，DDoS 攻击开始针对全球 DNS 服务器进行攻击，使得全球互联网服务一度

出现异常，后来还发生了针对 Google、Baidu 等搜索引擎的攻击。

攻击者通常使用一台主机控制一系列被感染的主机，通过这些主机发起大量的攻击流量。通常我们将这些被感染的主机称为“Botnet”(僵尸网络)，如图 9-30 所示。

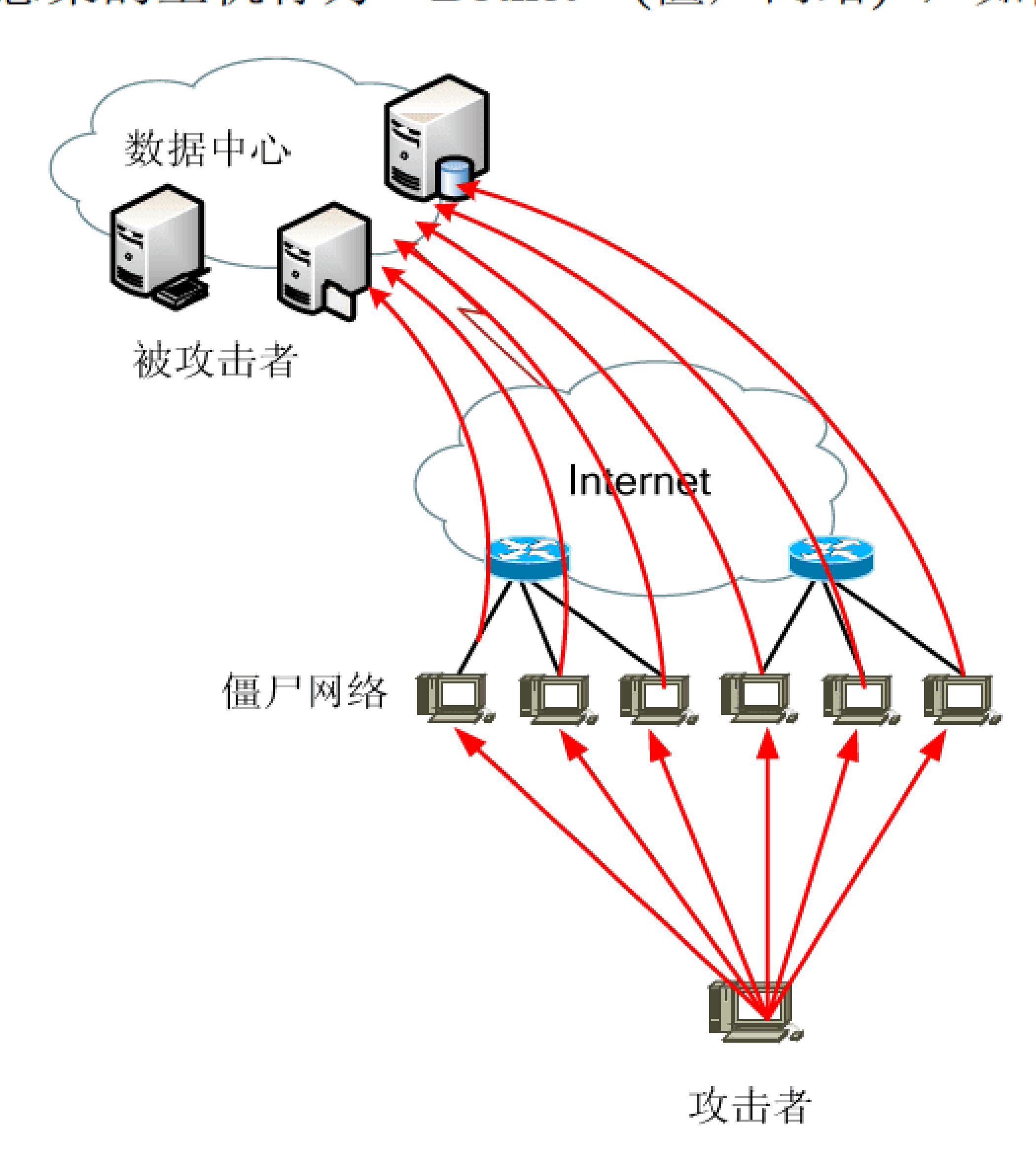


图 9-30　DDoS 攻击实例图

9.4.2　传统的 DDoS 防御方式

1. 防御 Trinoo

Trinoo 的攻击方法是向被攻击目标主机的随机端口发出全零的 4 字节 UDP 包，在处理这些超出其处理能力的垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，乃至崩溃。它对 IP 地址不做假，采用的通信协议和端口号如表 9-1 所示。

表 9-1 Trinoo 的攻击通信协议与端口号

通　信	传输层协议	端口号
攻击者主机到主控端主机	TCP	27665
主控端主机到代理端主机	UDP	27444
代理端主机到主服务器主机	UDP	31335

下面是在路由器上通过一个命名扩展 IP 访问控制列表来防御 Trinoo 攻击的例子。

```
Router(config)# ip access-list extended trinoo
Router(config-ext-nacl)# deny tcp any any eq 1524
Router(config-ext-nacl)# deny tcp eq 1524 any any
Router(config-ext-nacl)# deny udp eq 1524 any any
Router(config-ext-nacl)# deny tcp any any eq 27665
```

```
Router(config-ext-nacl)# deny tcp any eq 27665 any
Router(config-ext-nacl)# deny udp any any eq 27444
Router(config-ext-nacl)# deny udp any eq 27444 any
Router(config-ext-nacl)# deny udp any any eq 31335
Router(config-ext-nacl)# deny udp any eq 31335 any
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group trinoo out
Router(config-if)# ip access-group trinoo in
```

2. 防御 TFN

TFN 由主控端程序和代理端程序两部分组成，它主要采取的攻击方法为 SYN Flood、Ping Flood、UDP 炸弹和 SMURF，具有伪造数据包的能力。其中，SYN Flood 应对当前最流行的 DoS(拒绝服务攻击)与 DDoS(分布式拒绝服务攻击)的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽(CPU 满负荷或内存不足)的攻击方式。对于 SYN Flood 攻击，目前尚没有很好的监测和防御方法，不过如果系统管理员熟悉攻击方法和系统架构，通过一系列的设定，也能从一定程度上降低被攻击系统的负荷，减轻负面的影响。

下面是在路由器上通过一个命名扩展 IP 访问控制列表来防御 TFN 的例子。

```
Router(config)# ip access-list extended TFN-in
Router(config-ext-nacl)# permit icmp any host 10.0.0.1 echo-reply
Router(config-ext-nacl)# deny icmp any any echo-reply
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended TFN-out
Router(config-ext-nacl)# deny icmp any any echo-reply
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group TFN-out out
Router(config-if)# ip access-group TFN-in in
```

3. 防御 Stacheldraht

Stacheldraht 是从 TFN 派生出来的，因此它具有 TFN 的特性。此外它增加了主控端与代理端的加密通信能力，它对命令源做假，可以防范一些路由器的 RFC2267 过滤。Stacheldraht 中有一个内嵌的代理升级模块，可以自动下载并安装最新的代理程序。

下面是在路由器上通过一个命名扩展 IP 访问控制列表来防御 Stacheldraht 攻击的例子。

```
Router(config)# ip access-list extended Stacheldraht-in
Router(config-ext-nacl)# permit icmp any host 10.0.0.1 echo-reply
Router(config-ext-nacl)# deny icmp any any echo-reply
Router(config-ext-nacl)# deny tcp any any eq 16660
Router(config-ext-nacl)# deny tcp any eq 16660 any
Router(config-ext-nacl)# deny tcp any any eq 65000
Router(config-ext-nacl)# deny tcp any eq 65000 any
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended Stacheldraht-out
Router(config-ext-nacl)# deny icmp any any echo-reply
Router(config-ext-nacl)# deny tcp any any eq 16660
Router(config-ext-nacl)# deny tcp any eq 16660 any
Router(config-ext-nacl)# deny tcp any any eq 65000
Router(config-ext-nacl)# deny tcp any eq 65000 any
```

```
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group Stacheldraht-out out
Router(config-if)# ip access-group Stacheldraht-in in
```

4. 防御 Trinity

Trinity 联合了 Trinoo、TFN2K、Stacheldraht、Shaft 和其他程序，启动分布式拒绝服务(DDoS)攻击。DDoS 攻击是指攻击者将软件秘密嵌入成百上千台计算机，在特定命令或时间下，让受感染主机向目标机器发送消息。由 Internet 发来的大量消息能够有效地耗竭了目标服务器，使 Web 站点无法被其他网络用户访问。DDoS 曾经导致主要 Internet 厂商如 Yahoo 和 Amazon 等公司的 Web 站点临时关闭。

下面是在路由器上，通过一个命名扩展 IP 访问控制列表来防御 Trinity 的例子。

```
Router(config)# ip access-list extended trinity
Router(config-ext-nacl)# deny tcp any any range 6665 6669
Router(config-ext-nacl)# deny tcp any range 6665 6669 any
Router(config-ext-nacl)# deny tcp any any eq 33270
Router(config-ext-nacl)# deny tcp any eq 33270 any
Router(config-ext-nacl)# deny tcp any any eq 39168
Router(config-ext-nacl)# deny tcp any eq 39168 any
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group trinity out
Router(config-if)# ip access-group trinity in
```

5. 防御 SQL Slammer Worm

SQL Slammer Worm 是一个新的 Internet 蠕虫病毒，此病毒利用了微软 SQL Server 2000 的远程堆栈缓冲区溢出漏洞，主要攻击 Windows 操作系统中的 SQL Server 2000 服务器。

SQL 的 UDP 的 1434 端口主要用于客户端查询可用的连接方式，但由于程序上的漏洞，当客户端发送超长数据包时，将导致缓冲区溢出，恶意黑客便利用此漏洞在远程机器上执行准备好的恶意代码，将病毒放到 Internet 上。感染病毒的机器将不断向外发送这种 UDP 数据包造成网络堵塞。

下面是在路由器上，通过一个命名扩展 IP 访问控制列表来防御 SQL Slammer Worm 的例子。

```
Router(config)# ip access-list extended slammer
Router(config-ext-nacl)# deny udp any any eq 1434
Router(config-ext-nacl)# deny tcp any any eq 1433
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group slammer in
Router(config-if)# ip access-group slammer out
```

6. 防御微软 RPC 漏洞攻击

Remote Procedure Call(RPC)是 Windows 操作系统使用的一种远程过程调用协议。RPC 协议提供一种进程间的交互通信机制，允许本地机器上的程序进程无缝地在远程系统中运行代码。由于部分 RPC 在使用 TCP/IP 协议处理信息交换时，不能正确地处理畸形的消息从而导致存在一个安全漏洞。该漏洞影响使用 RPC 的 DCOM 接口，这个接口用来处理由客户

端机器发送给服务器的 DCOM 对象激活请求(如 UNC 路径)。下面是在路由器上，通过一个命名扩展 IP 访问控制列表来防御微软 RPC 漏洞攻击的例子。

```
Router(config)# ip access-list extended ms-rpc
Router(config-ext-nacl)# deny tcp any any eq 135
Router(config-ext-nacl)# deny udp any any eq 135
Router(config-ext-nacl)# deny udp any any range 137 139
Router(config-ext-nacl)# deny tcp any any eq 139
Router(config-ext-nacl)# deny tcp any any eq 445
Router(config-ext-nacl)# deny tcp any any eq 593
Router(config-ext-nacl)# deny tcp any any eq 4444
Router(config-ext-nacl)# exit
Router(config)# interface Gi1/0
Router(config-if)# ip access-group ms-rpc in
Router(config-if)# ip access-group ms-rpc out
```

7. 利用 CBAC 防御 DDoS

基于内容的访问控制(CBAC)是对 Cisco 传统访问列表的扩展，它基于应用层会话信息，能够智能地过滤 TCP 和 UDP 数据包，防止 DDoS 攻击。

CBAC 通过设置超时限值和会话门限值来决定会话的维持时间以及何时删除半连接。对于 TCP 而言，半连接是指一个没有完成三阶段握手过程的会话。对 UDP 而言，半连接是指路由器没有检测到返回流量的会话。

CBAC 正是通过监视半连接的数量和产生的频率来防止洪水攻击。每当有不正常的半连接建立或者在短时间内出现大量半连接的时候，用户可以判断是否遭受了洪水攻击。CBAC 每分钟检测一次已经存在的半连接数量和试图建立连接的频率，当已经存在的半连接数量超过了门限值，路由器就会删除一些半连接，以保证新建立连接的需求。同样，当试图建立连接的频率超过门限值，路由器就会采取相同的措施，删除一部分连接请求。通过这种连续不断的监视和删除，CBAC 可以有效防止 SYN Flood 和 Fraggle 攻击。

下面是利用 CBAC 防止 DDoS 的配置过程。

❶ 设置一些门限值，超过门限值时路由器就会删除一些半连接。

```
Router(config)# ip inspect tcp synwait-time 20
Router(config)# ip inspect tcp idle-time 60
Router(config)# ip inspect udp idle-time 20
Router(config)# ip inspect max-incomplete high 400
Router(config)# ip inspect max-incomplete low 300
Router(config)# ip inspect one-minute high 600
Router(config)# ip inspect one-minute low 500
Router(config)# ip inspect tcp max-incomplete host 300  block-time 0
```

❷ 配置对半开放连接的限制，以控制 DDoS 攻击。

```
Router(config)#access-list 100 permit ip any host 192.168.1.1
Router(config)#ip tcp intercept list 100
Router(config)#ip tcp intercept max-incomplete high 10
Router(config)#ip tcp intercept one-minute high 15
Router(config)#ip tcp intercept max-incomplete low 5
Router(config)#ip tcp intercept one-minute low 10
```

❸ 对丢弃模式等进行控制。

```
Router(config)#ip tcp intercept drop-mode random
```

```
Router(config)#ip tcp intercept watch-timeout 15
Router(config)#ip tcp intercept mode watch
```

9.4.3 新型 DDoS 保护策略

传统的 DDoS 防御方式过于被动，仅限于对已有的一些攻击进行过滤。国内外众多厂商生产的防火墙(如 NetScreen-100、Fortigate-300、Nokia Firewall-I 等)仅能承受 30～40Mbps 的流量，而一台普通 P3800 的 PC 在 Linux 环境下可以产生 50Mbps 的 DDoS 流量。即便是一些千兆硬件防火墙(如 Netscreen-Giga、Fortigate-2000、天融信等)也无法抵挡大量的攻击，从而导致防火墙瘫痪，全网中断。

新型的 DDoS 防御系统通常采用多级流量异常检测的方法进行流量过滤，通常国内的一些厂商使用串行模式进行异常过滤，如图 9-31 所示。

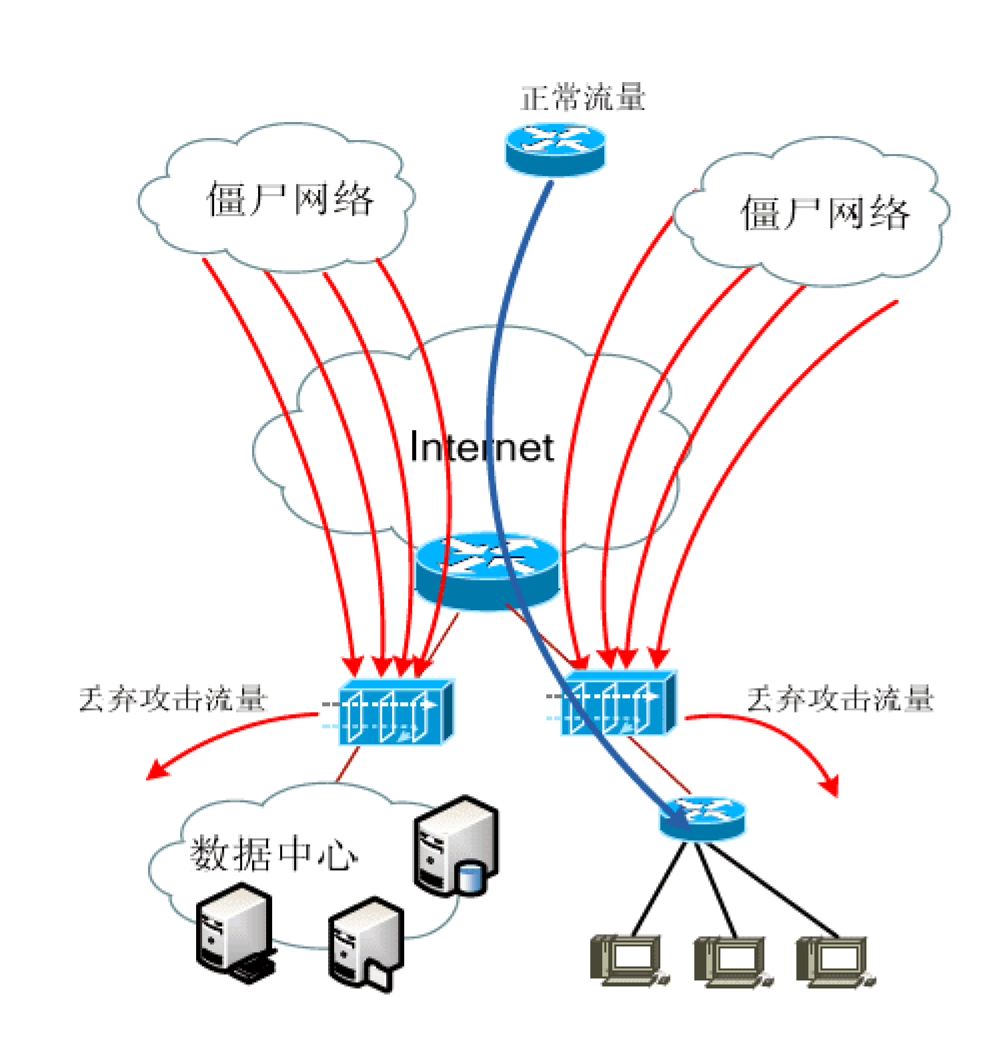


图 9-31 串行 DDoS 过滤设备

串行部署方式可以不需要 DDoS 攻击检测设备，直接放置于需要防护的设备前端。但这样的部署方式对于大规模部署，需要较多的投资，同时在大流量攻击下，这类设备通常容易产生性能瓶颈，如果攻击使这些设备瘫痪，正常业务也会中断。

串行的流量过滤方式还有一个缺点是仅能看到局部流量的异常情况，无法追踪攻击源，并在有效的位置进行攻击流量过滤。因此现在很多厂商开始支持基于旁挂模式的 DDoS 过滤系统。旁挂式系统通常由两个组件构成，一个是过滤器，另一个是检测器。Cisco、绿盟等厂商的 DDoS 防范解决方案采用的是这种方式。如图 9-32 所示。

Cisco 提供了 Detector 和 Guard 两种设备用于 DDoS 过滤，Detector 通过旁挂在受保护的设备上进行流量检测，当出现攻击后，将消息通过 SSH 传送到 Guard，Guard 通过 BGP 路由协议发送通告给前端路由器，将攻击流量引入 Guard 丢弃。除了 BGP 路由回送外，Cisco 还支持 VRF、GRE、L2TP 等方式，适合运营商用户。除了提供使用 IBM X345 服务器平台的外置异常检测和异常过滤设备外，Cisco 还在 Catalyst 6500 和 7600 上提供了内置的模块，

极大地提高了设备的安全性，如图 9-33 所示。

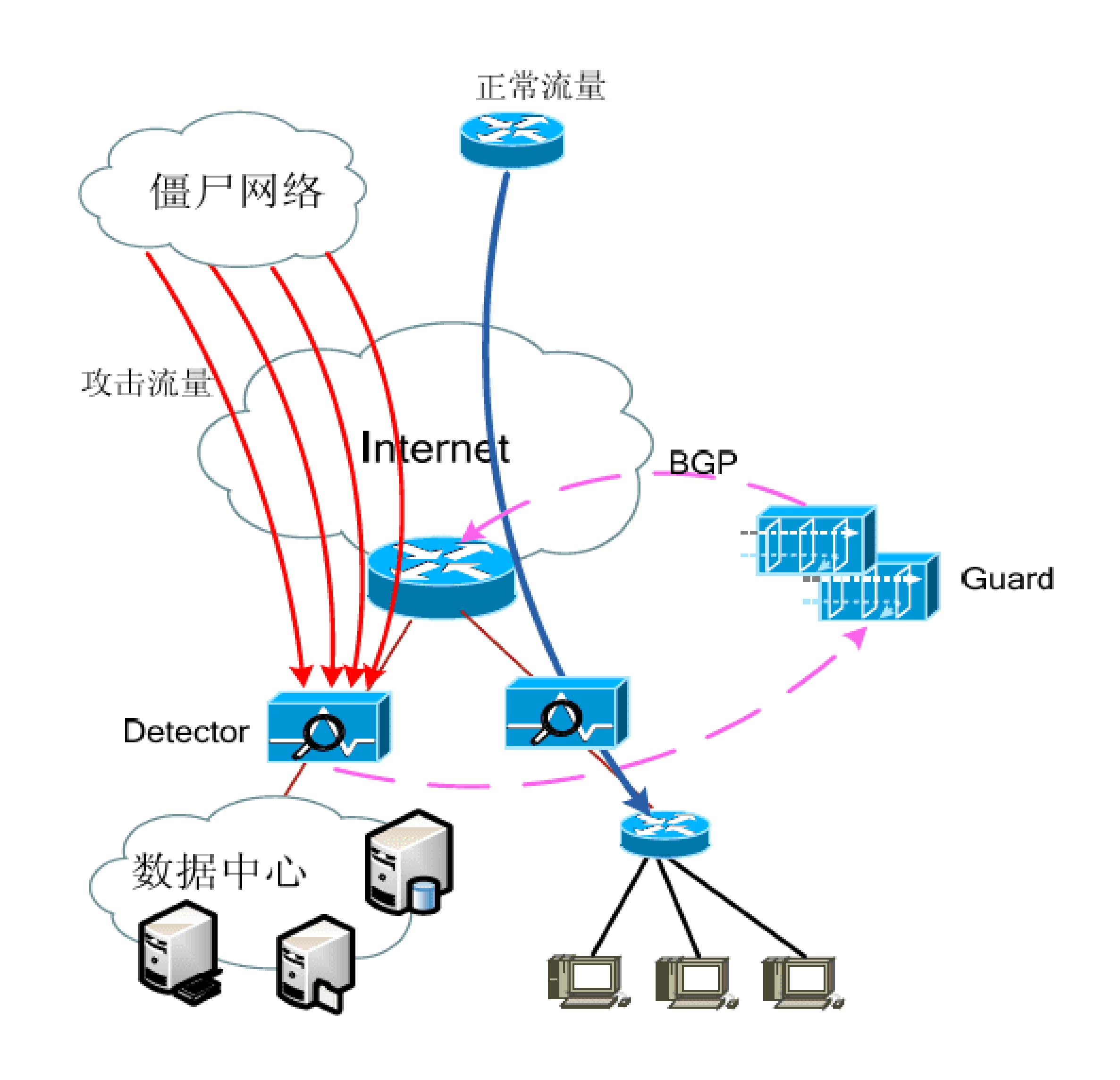


图 9-32　旁挂 DDoS 过滤设备



图 9-33　Cisco DDoS 防御设备

除了使用 Cisco 专用的 DDoS Traffic Anomaly Detector 外，还可以使用基于 NetFlow 的方式进行流量监控。NetFlow 可以统计记录网络中数据包的源目的地址、端口号等信息，将这些信息收集整理分析后，就可以发现网络通信的规律。在 Cisco 多数的路由交换设备中，有专门的硬件芯片和软件特性实现 NetFlow。而最新的 NetFlow 9 已被选中参与 IETF 标准，在成为标准前，这一技术已经得到了业界广泛的支持，用户可以找到很多家厂家提供的收集交换机路由器 NetFlow 信息、汇总分析的软件。用户甚至可以找到开放源代码或者免费的软件来收集分析 NetFlow 信息，如图 9-34 所示。因此，对于运营商而言，通常使用 NetFlow 的方式进行异常流量检测和 DDoS 攻击防御。

Arbor Networks PeakFlow SP(http://www.arbornetworks.com/)是一个可扩展的平台，可以提供一个全面的解决方案，为电信运营商及其客户提供强大的 DDoS 检测防御、流量和路由功能。PeakFlow SP 能让电信运营商可以为他们的企业客户提供可扩展的 DDoS 检测防御和流量管理工具，也可以帮助网络管理人员主动地检测和清除整个网络中的异常情况，例如 DDoS 攻击和蠕虫。PeakFlow SP 的流量和路由功能可以分析流量网络，让操作人员可以及时地针对路由、传输、合作伙伴和客户制定业务决策，如图 9-35 所示。

Protocol	TotalFlows	Flow /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telent	2656855	4.3	86	78	372.3	49.6	27.6
TCP-FTP	5900082	9.5	9	71	86.8	11.4	33.1
TCP-FTPD	3200453	5.1	193	461	1006.3	45.8	33.4
TCP-WWW	546778274	887.3	12	325	11170.8	8.0	32.3
TCP-SMTP	25536863	41.4	21	283	876.5	10.9	31.3
TCP-X	116391	0.1	231	269	43.8	68.2	27.3
TCP-BGP	24520	0.0	28	216	1.1	26.2	39.0
TCP-Frag	56847	0.0	24	952	2.2	13.1	33.2
TCP-other	49148540	79.7	47	338	3752.6	30.7	32.2
UDP-DNS	117240379	190.2	3	112	570.8	7.5	34.7
UDP-NTP	9378269	15.2	1	76	16.2	2.2	38.7
UDP-TFTP	8077	0.0	3	62	0.0	9.7	33.2
UDP-Frag	51161	0.0	14	322	1.2	11.0	39.4
UDP-other	45502422	73.8	30	174	2272.7	8.5	37.8
ICMP	14837957	24.0	5	224	125.8	12.1	34.3
IGMP	40916	0.0	170	207	11.3	197.3	13.5
IPINIP	3988	0.0	48713	393	315.2	644.2	19.6
GRE	3838	0.0	79	101	0.4	47.3	25.9
IP-other	77406	0.1	47	259	5.9	52.4	27.0
Total	820563238	1331.7	15	304	20633.0	9.8	33.0

图 9-34　NetFlow 生成的报表



图 9-35　Arbor PeakFlow

PeakFlow SP 可以利用它的双层收集器架构进行扩展。这些收集器可以从多个路由器和一个控制器获取 NetFlow 统计数据。控制器可以协调事件关联和对事件进行追溯。当 PeakFlow SP 与 Cisco Guard 结合提供 DDoS 防御功能时，一旦通过收集器获得某个区域的异常信息，控制器就会建立 SSH 连接，启用 Cisco Guard，将受攻击区域置于保护模式。

运营商基于 Arbor PeakFlow SP 和 Cisco Guard XT 的部署方式如图 9-36 所示。

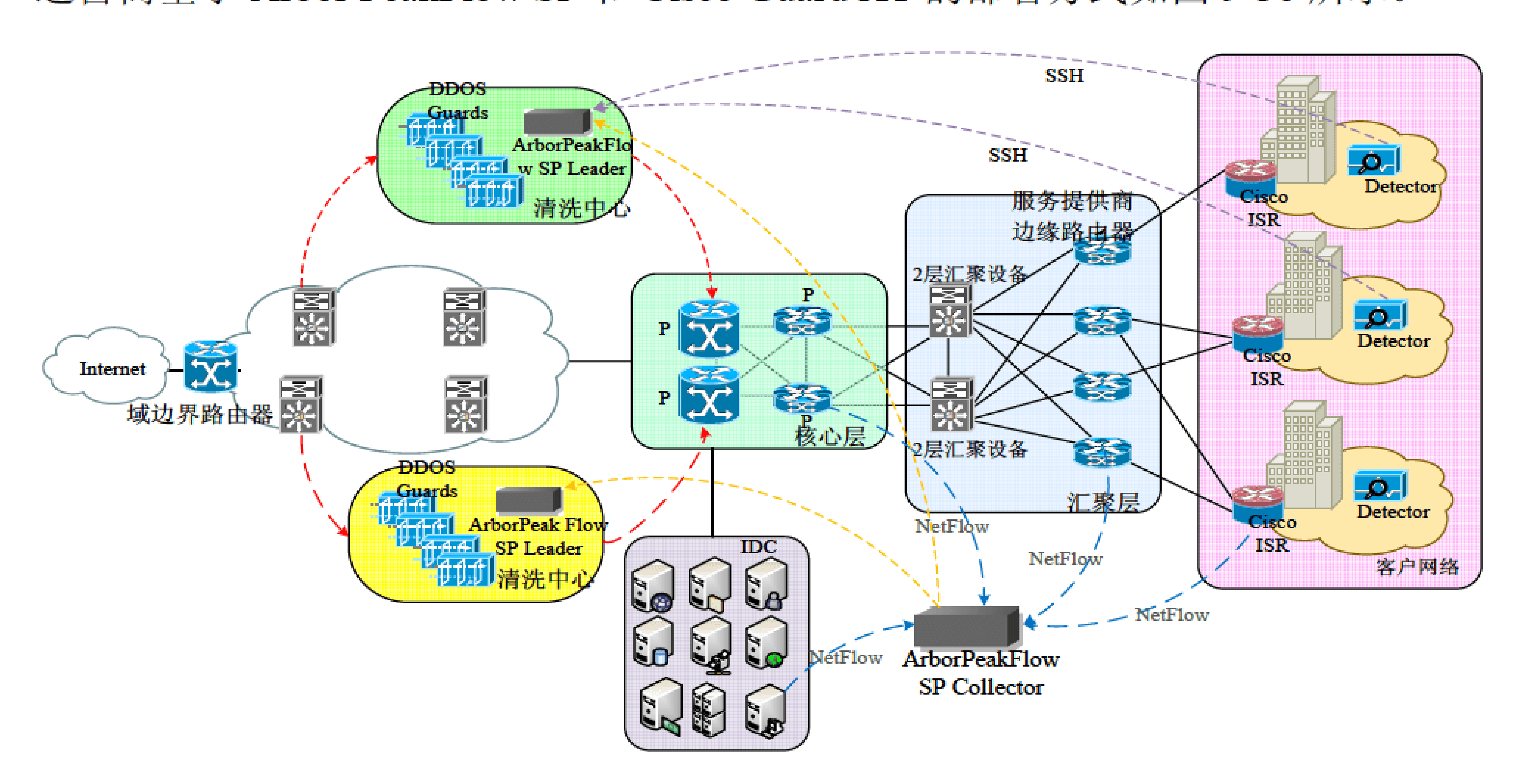


图 9-36　DDoS 防御系统(基于 Arbor PeakFlow 和 Cisco Guard XT)

通常运营商还可以使用的方式，使用 PeakFlow SP 托管用户网络的 NetFlow 数据，并建立多个较大的清洗中心集中清洗攻击流量。客户端仅需按如下方式配置 NetFlow，并指向 Arbor PeakFlow SP 即可。

```
Router(config)#ip flow-export source GigabitEthernet0/1
Router(config)#ip flow-export destination 192.168.1.1 5544
Router(config)#ip flow-export version 5
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config)#interface GigabitEthernet 0/2
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
```

但是，基于 NetFlow 的检测方式还存在一些漏洞。一是 NetFlow 的 DDoS 监测功能不如 Detector 那样准确。Detector 是每包检查，而 NetFlow 只是数一个总的数据包的个数，甚至是做取样的。对于很多包个数变化并不明显的攻击(称之为 low-rate 攻击)和一些基于应用的攻击，NetFlow 就无能为力。二是 NetFlow 通常按一定的时间间隔传送到 Arbor PeakFlow，对于一些实效性较强的应用无法及时的作出响应。

📖**点评与拓展：**随着互联网的迅猛发展，攻击手法已经出现明显的集团化趋势，特别是最近的很多 DDoS 攻击，具有明显的目的性。而这样的攻击触发仅需极少的金钱就可以获得一个规模庞大的僵尸网络。因此互联网 DDoS 攻击防御成为网络安全中非常重要的因素。对于一些内容服，务提供商和电子商务运营商而言，它们将非常需要这样的设备来维护其网络安全。

9.5 本 章 小 结

本章介绍了入侵检测及相应的防御策略以及 IPS/IDS 的工作原理，并介绍了 Cisco IOS IPS、AIP-SSM、IDSM-2 以及 IPS 4200 系列产品的配置方法，还介绍了基于 IDM 的配置方式。之后，介绍了基于 Linux 的 IDS 配置，通过 SNORT 和 ACID 的结合构建了一种免费的入侵检测平台，但是其检测规则升级较为不便。在本章的最后部分，介绍了常见的 DDoS 攻击以及防御 DDoS 攻击的方法。下一章我们将介绍用户远程接入网络的一些安全性配置。

第 10 章　远 程 访 问

通常，很多公司的分支机构希望使用一种安全的方式访问总部的网络，但这些链路通常需要通过 Internet，如果不使用相应的加密措施，数据安全性很难保障。同时，很多公司希望给员工创造远程办公的环境，因此也需要为员工提供安全的远程访问机制。

通过本章的学习，读者应掌握以下主要内容：

- ✧ IPSec VPN
- ✧ SSL VPN
- ✧ 配置基于 ISA Server 2004 VPN
- ✧ 配置 Linux VPN

10.1　VPN 概述

10.1.1　VPN 简介

虚拟专用网络(VPN)是一种新型的网络技术，它为我们提供了一种通过公用网络(如最大的公用因特网)安全地对企业内部专用网络进行远程访问的连接方式。我们知道一个网络连接通常由 3 个部分组成：客户机、传输介质和服务器。VPN 网络同样也需要这 3 部分，不同的是 VPN 连接不是采用物理的传输介质，而是使用一种称为“隧道”的东西来作为传输介质的，这个隧道是建立在公共网络或专用网络基础之上的，例如因特网或专用 Intranet 等。同时，要实现 VPN 连接，企业内部网络中必须配置一台基于 Windows NT、Windows 2000 Server 或 Windows Server 2003 的 VPN 服务器，或者使用一台支持 VPN 功能的防火墙或路由器来充当 VPN 服务器。VPN 服务器一方面连接企业内部专用网络(LAN)，另一方面要连接到因特网或其他专用网络，这就要 VPN 服务器必须拥有一个公用的 IP 地址，也就是说企业必须先拥有一个合法的 Internet 或专用网域名。当客户机通过 VPN 连接与专用网络中的计算机进行通信时，先由 NSP(网络服务提供商)将所有的数据传送到 VPN 服务器，然后再由 VPN 服务器将所有的数据传送到目标计算机。因为在 VPN 隧道中通信能确保通信通道的专用性，并且传输的数据是经过压缩、加密的，所以 VPN 通信同样具有专用网络的通信安全性。

10.1.2　VPN 分类

1. GRE

GRE(Generic Routing Encapsulation，路由封装)主要用于源路由和终路由之间所形成的

隧道。例如，将通过隧道的报文用一个新的报文头(GRE 报文头)进行封装然后带着隧道终点地址放入隧道中。当报文到达隧道终点时，GRE 报文头被剥掉，继续按原始报文的目标地址进行寻址。GRE 隧道通常是点到点的，即隧道只有一个源地址和一个终地址。然而也有一些实现允许点到多点，即一个源地址对多个终地址。这时候就要和下一跳路由协议(Next-Hop Routing Protocol，NHRP)结合使用。NHRP 主要是为了在路由之间建立捷径。

GRE 隧道用来建立 VPN 有很大的吸引力。从体系结构的观点来看，VPN 就像是通过普通主机网络的隧道集合。普通主机网络的每个点都可利用其地址以及路由所形成的物理连接，配置成一个或多个隧道。在 GRE 隧道技术中，入口地址用的是普通主机网络的地址空间，而在隧道中流动的原始报文用的是 VPN 的地址空间，这样反过来就要求隧道的终点应该配置成 VPN 与普通主机网络之间的交界点。这种方法的好处是使 VPN 的路由信息从普通主机网络的路由信息中隔离出来，多个 VPN 可以重复利用同一个地址空间而没有冲突，这使得 VPN 从主机网络中独立出来，从而满足了 VPN 的关键要求：可以不使用全局唯一的地址空间。隧道也能封装数量众多的协议族，减少实现 VPN 功能函数的数量。还有，对许多 VPN 所支持的体系结构来说，用同一种格式来支持多种协议同时又保留协议的功能，这是非常重要的。IP 路由过滤的主机网络不能提供这种服务，而只有隧道技术才能把 VPN 私有协议从主机网络中隔离开来。基于隧道技术的 VPN 实现的另一特点是对主机网络环境和 VPN 路由环境进行隔离。对 VPN 而言主机网络可看成点到点的电路集合，VPN 能够用其路由协议穿过符合 VPN 管理要求的虚拟网。同样，主机网络使用符合网络要求的路由设计方案，而不必受 VPN 用户网络的路由协议限制。

虽然 GRE 隧道技术有很多优点，但使用其技术作为 VPN 机制也有缺点，例如管理费用高、隧道的规模数量大等。因为 GRE 是由手工配置的，所以配置和维护隧道所需的费用与隧道的数量是直接相关的——每次隧道的终点改变，隧道都要重新配置。隧道也可自动配置，但存在缺点，例如不能考虑相关路由信息、性能问题以及容易形成回路问题。一旦形成回路，会极大恶化路由的效率。除此之外，通信分类机制是通过一个好的粒度级别来识别通信类型。如果通信分类过程是通过识别报文(进入隧道前的)进行的话，就会影响路由发送速率的能力及服务性能。

GRE 隧道技术是用在路由器中的，可以满足 Extranet VPN 以及 Intranet VPN 的需求。但是在远程访问 VPN 中，多数用户是采用拨号上网，这时可以通过 L2TP 和 PPTP 来加以解决。

2. L2TP/PPTP

L2TP 是 L2F(Layer 2 Forwarding，第二层转发)和 PPTP 的结合。由于 PC 机的桌面操作系统包含着 PPTP，因此 PPTP 仍比较流行。隧道的建立有两种方式：用户初始化隧道和 NAS(Network Access Server，网络接入服务器)初始化隧道。前者一般指“主动”隧道，后者指“强制”隧道。“主动”隧道是用户为某种特定目的的请求建立的，而“强制”隧道则是在没有任何来自用户的动作以及选择的情况下建立的。

L2TP 作为“强制”隧道模型是让拨号用户与网络中的另一点建立连接的重要机制，其建立过程如下。

(1) 用户通过 Modem 与 NAS 建立连接。

(2) 用户通过 NAS 的 L2TP 接入服务器身份认证。

(3) 在政策配置文件或 NAS 与政策服务器进行协商的基础上，NAS 和 L2TP 接入服务器动态地建立一条 L2TP 隧道。

(4) 用户与 L2TP 接入服务器之间建立一条点到点协议(Point to Point Protocol，PPP)访问服务隧道。

(5) 用户通过该隧道获得 VPN 服务。

与之相反的是，PPTP 作为"主动"隧道模型允许终端系统进行配置，与任意位置的 PPTP 服务器建立一条不连续的、点到点的隧道。而且，PPTP 协商和隧道建立过程都没有中间媒介 NAS 的参与。NAS 的作用只是提供网络服务。PPTP 的建立过程如下。

(1) 用户通过串口以拨号 IP 访问的方式与 NAS 建立连接取得网络服务。

(2) 用户通过路由信息定位 PPTP 接入服务器。

(3) 用户形成一个 PPTP 虚拟接口。

(4) 用户通过该接口与 PPTP 接入服务器协商、认证建立一条 PPP 访问服务隧道。

(5) 用户通过该隧道获得 VPN 服务。

在 L2TP 中，用户感觉不到 NAS 的存在，仿佛与 PPTP 接入服务器直接建立连接。而在 PPTP 中，PPTP 隧道对 NAS 是透明的；NAS 不需要知道 PPTP 接入服务器的存在，只是简单地把 PPTP 流量作为普通 IP 流量处理。

采用 L2TP 还是 PPTP 实现 VPN 取决于要把控制权放在 NAS 还是用户手中。L2TP 比 PPTP 更安全，因为 L2TP 接入服务器能够确定用户从哪里来的。L2TP 主要用于比较集中的、固定的 VPN 用户，而 PPTP 比较适合移动的用户。

3. IPSec

IPSec(IP Security，IP 安全)是指 IETF 以 RFC 形式公布的一组安全 IP 协议集，是在 IP 包级为 IP 业务提供保护的安全协议标准，其基本目的就是把安全机制引入 IP 协议，通过使用现代密码学方法支持加密性和认证性服务，使用户能有选择地使用并得到所期望的安全服务。

- ✧ 私有性：IPSec 在传输数据包之前将其加密，以保证数据的私有性；
- ✧ 完整性：IPSec 在目的地要验证数据包，以保证该数据包在传输过程中没有被修改；
- ✧ 真实性：IPSec 端要验证所有受 IPSec 保护的数据包；
- ✧ 防重放：IPSec 防止了数据包被捕捉并重新投放到网上，目的地会拒绝旧的或重复的数据包，这通过报文的序列号实现；

4. SSL VPN

安全套接层协议(Secure Socket Layer，SSL)是由 Netscape 设计的一种开放性协议，它提供了一种介于应用层和传输层之间的数据安全套接层协议机制。它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性，以及可选的客户机认证。SSL 是在 Internet 基础上提供的一种保证私密性的安全协议，它能使客户机/服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 协议要求建立在可靠的传输层协议(如 TCP)之上。SSL 协议的优势在于它是与应用层协议独立无关的。高层的应用层协议(如

HTTP、FTP、TELNET 等)能透明地建立在 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商，以及服务器认证工作。在此之后，应用层协议所传送的数据都会被加密，从而保证通信的私密性。

SSL 协议提供的安全信道有以下 3 个特性。

✧ 私密性：在握手协议定义了会话密钥后，所有的消息都被加密。
✧ 确认性：尽管会话的客户端认证是可选的，但是服务器端始终是被认证的。
✧ 可靠性：传送的消息包括消息完整性检查(使用 MAC)。

所谓的 SSL VPN，其实是 VPN 设备厂商为了与 IPsec VPN 区别所创造出来的名词，指的是使用者利用浏览器内建的 SSL 封包处理功能，用浏览器连回公司内部 SSL VPN 服务器，然后通过网络封包转向的方式，让使用者可以在远程计算机执行应用程序，读取公司内部服务器数据。它采用标准的 SSL 对传输中的数据包进行加密，从而在应用层保护了数据的安全性。高质量的 SSL VPN 解决方案可保证企业进行安全的全局访问。在不断扩展的互联网 Web 站点之间、远程办公室、传统交易大厅和客户端间，SSL VPN 克服了 IPSec VPN 的不足，用户可以轻松实现安全易用、无须客户端安装且配置简单的远程访问，从而降低用户的总成本并增加远程用户的工作效率。而同样在这些地方，设置传统的 IPSec VPN 非常困难，甚至是不可能的，因为必须更改网络地址转换(NAT)和防火墙设置。

10.1.3 IPSec VPN 和 SSL VPN 的比较

SSL VPN 与 IPSec VPN 是目前流行的两类 Internet 远程安全接入技术，它们具有类似的功能特性，但也存在很大不同。

SSL 的“零客户端”解决方案被认为是实现远程接入的最大优势，这对缺乏维护大型 IPSec 配置资源的用户来说的确如此。但 SSL 方案也有不足，它仅支持以代理方式访问基于 Web 或特定的客户端/服务器的应用。由服务器直接操纵的应用，例如 Net Meeting 及一些客户书写的应用程序，将无法进行访问。

1. IPSec 方案的安全级别高

基于 Internet 实现多专用网安全连接，IPSec VPN 是比较理想的方案。IPSec 工作于网络层，对终端站点间所有传输数据进行保护，而不管是哪类网络应用。它在事实上将远程客户端“置于”企业内部网，使远程客户端拥有内部网用户一样的权限和操作功能。

IPSec VPN 要求在远程接入客户端适当安装和配置 IPSec 客户端软件和接入设备，这大大提高了安全级别，因为访问受到特定的接入设备、软件客户端、用户认证机制和预定义安全规则的限制。

IPSec VPN 还能减轻网管负担。如今一些 IPSec 客户端软件能实现自动安装，不需要用户参与。VPN 服务能够自动安装终端用户接入设备和配置客户端软件包，因而无论对网管还是终端用户，安装过程都大为简化。

2. IPSec VPN 应用优势

SSL 用户仅限于运用 Web 浏览器接入，这对新型的基于 Web 的商务应用软件比较合适，

但它限制了非 Web 应用访问，使得一些文件操作功能难于实现，例如文件共享、预定文件备份和自动文件传输。用户可以通过升级、增加补丁、安装 SSL 网关或其他办法来支持非 Web 应用，但实现成本高且复杂，难以实现。IPSec VPN 能顺利实现企业网资源访问，用户不一定要采用 Web 接入(可以是非 Web 方式)，这对同时需要以两种方式进行自动通信的应用程序来说是最好的方案。

IPSec 方案能实现网络层连接，任何 LAN 应用都能通过 IPSec 隧道进行访问，因而在用户仅需要网络层接入时，IPSec 是理想方案。如今，有的机构同时采用 IPSec 和 SSL 远程接入方案，管理员利用 IPSec VPN 实现网络层接入，进行网络管理；其他人员要访问的资源有限，一般也就是电子邮件、传真以及接入公司内部网(Web 浏览)，因而采用 SSL 方案。这正是充分利用了 IPSec 的网络层接入功能。

3. IPSec VPN 与 SSL VPN 优劣比较

IPSec VPN 和 SSL VPN 各有优缺点。IPSec VPN 提供完整的网络层连接功能，因而是实现多专用网安全连接的最佳选项；而 SSL VPN 的“零客户端”架构特别适合于远程用户连接，用户可通过任何 Web 浏览器访问企业网 Web 应用。SSL VPN 存在一定的安全风险，因为用户可运用公众 Internet 站点接入；IPSec VPN 需要软件客户端支撑，不支持公共 Internet 站点接入，但能实现 Web 或非 Web 类企业应用访问。

10.2　配置 IPSec VPN

应用实例导航：利用 IPSec VPN 提高分支机构链接安全性

※场景呈现

Sadness 公司随着业务的逐渐扩大，在很多城市建立了分公司，这些分公司如何有效而安全地连入总公司的核心网络成为一个难题，Sadness 公司远程办公网络拓扑结构如图 10-1 所示。

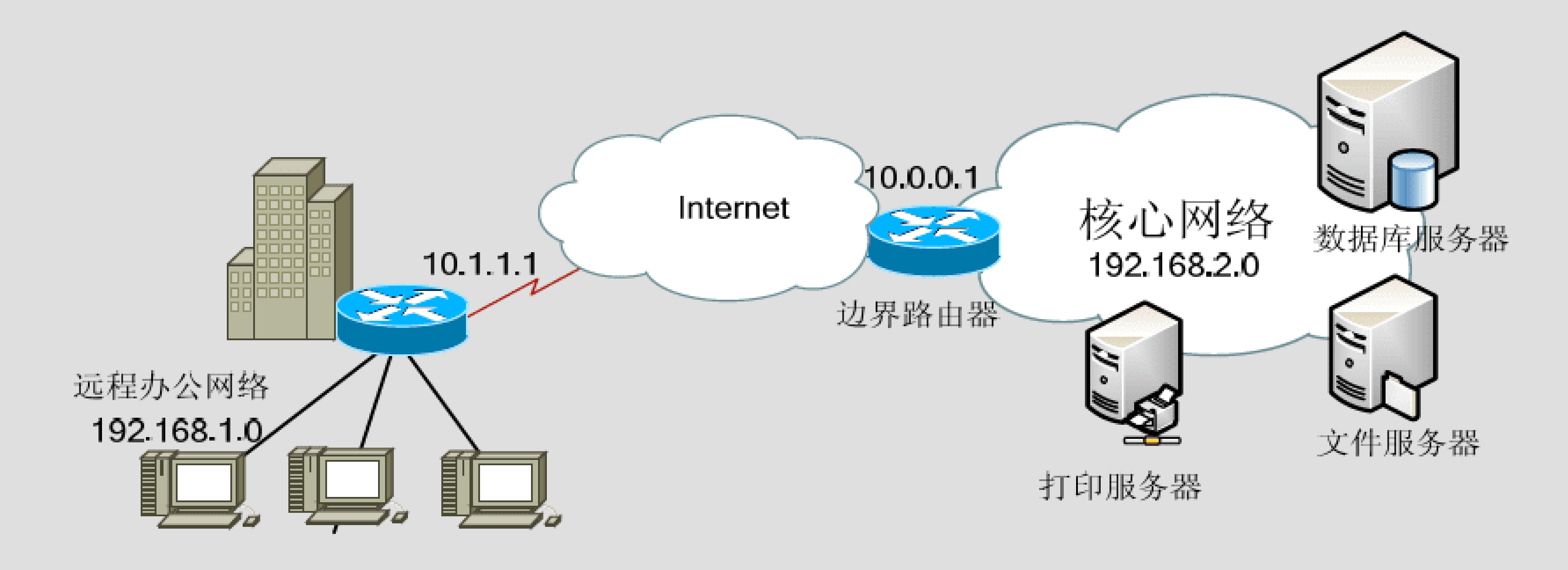


图 10-1　Sandess 远程办公网络拓扑图

Jam 为公司提出了使用 IPSec VPN 的配置方式，提供静态的站点到站点的安全访问方式。

※技术要领

(1) IPSec VPN 的基本工作原理；
(2) 配置基于预共享密钥认证的 IPSec VPN；
(3) 配置基于 CA 证书公钥认证的 IPSec VPN。

IPSec VPN 技术在 IP 传输上通过加密隧道，在用公网传送内部专网的内容的同时，保证内部数据的安全性，从而实现企业总部与各分支机构之间的数据、话音、视频业务互通。如今，许多企业已经把 VPN 作为远端分支和移动用户连接的主要手段来构建企业虚拟业务网。

10.2.1 IPSec VPN 概述

1. IPSec 的安全结构

IPSec 是在 IP 网络上保证安全通信的开放标准框架，实际上是一套协议包而不是单个的协议。IPSec 的安全结构包括 3 个基本部分：安全协议、安全关联和密钥管理协议。IPSec 独立于密码学算法，这使得不同的用户群可以选择不同的安全算法。

1) 安全协议

安全协议主要包括 AH(Authentication Header，认证头)协议和 ESP(Encapsulating Security Payload，封装安全载荷)协议。其中，AH 为 IP 数据包提供无连接的数据完整性和数据源身份认证。数据完整性通过消息认证码(如 MD5、SHA1)产生的校验值来保证，数据源身份认证通过在待认证的数据中加入一个共享密钥来实现，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。ESP 为 IP 数据包提供数据的保密性(通过加密机制)、无连接的数据完整性、数据源身份认证以及防重防攻击保护。AH 和 ESP 可以单独使用，也可以配合使用，通过组合可以配置多种灵活的安全机制。

IPSec 有隧道和传输两种工作方式。在隧道方式中，用户的整个 IP 数据包被用来计算附加报头，而且被加密，附加报头和加密用户数据被封装在一个新的 IP 数据包中；在传输方式中，只是传输层(如 TCP、UDP、ICMP)数据被用来计算附加报头，附加报头和被加密的传输层数据被放置在原 IP 报头后面。

2) 安全关联

两台 IPSec 主机在交换数据之前，必须首先建立某种约定，这种约定称为安全关联(Security Association，SA)，指双方需要就如何保护信息、交换信息等公用的安全设置达成一致，更重要的是必须有一种方法使那两台计算机安全地交换一套密钥，以便在它们的连接中使用。

IPSec 的安全关联可以通过手工配置的方式建立，但是当网络中结点增多时，手工配置将非常困难，而且难以保证安全性。这时就要使用 IKE 自动地进行安全关联建立与密钥交换的过程。

3) 密钥管理协议

IKE(Internet Key Exchange，因特网密钥交换)在通信双方之间建立安全关联，提供密钥

确定、密钥管理机制，是一个产生和交换密钥材料并协商 IPSec 参数的框架。IKE 将密钥协商的结果保留在 SA 中，供 AH 和 ESP 通信时使用。

2. IPSec 的工作过程

IPSec 的工作过程可以分成 5 个主要步骤。

(1)　IPSec 过程启动：根据配置 IPSec 对等体(如公司总部的路由器和分支机构的路由器)中的 IPSec 安全策略，指定要被加密的数据流，启动 IKE(Internet 密钥交换)过程；

(2)　IKE 阶段 1：在该连接阶段，IKE 认证 IPSec 对等体，协商 IKE 安全关联(SA)，并为协商 IPSec 安全关联的参数建立一个安全传输道路；

(3)　IKE 阶段 2：IKE 协商 IPSec 的 SA 参数，并在对等体中建立与之匹配的 IPSec SA；

(4)　数据传送：根据存储在 SA 数据库中的 IPSec 参数和密钥，在 IPSec 对等体间传送数据；

(5)　IPSec 隧道终止：通过删除或超时机制结束 IPSec SA。

10.2.2　配置 IPSec VPN

为了验证对方的合法性，只有通过认证系统才可以建立 VPN 通信连接。IPSec VPN 有两种认证方法：预共享密钥(Pre-shared Key)认证和基于 CA 证书的公钥认证。下面分别介绍这两种认证方法在 Cisco 路由器中的配置过程。

1. 使用预共享密钥认证

在使用预共享密钥时，VPN 会话双方都配置了一个预置的密钥。会话的双方并不真正将这个密钥传输给对方。相反，当会话的一方初始化一个 VPN 通道时，会进行一个分成两个阶段的 IKE。在第一阶段，IKE 使用预共享密钥和 Diffie-Hellman 算法生成一个会话密钥。这个会话密钥可以用于会话双方彼此之间的认证和保护通信通道的安全。

一旦通信通道建立起来了，IKE 在第二阶段协商一个 IPSec 安全组合。这个安全组合为 VPN 会话的双方建立一个公共的配置方案，用于加密它们之间传输的数据。在第二阶段，IKE 生成一个会话密钥。因为第二阶段比第一阶段持续时间长得多，IKE 定期重新生成第二阶段会话密钥。

与手工密钥相比，预共享密钥的优势是网络管理员的管理更加容易一些。然而，一个预共享密钥配置可能降低传输效率，特别是如果频繁生成第二阶段密钥的话。

下面的操作是采用预共享密钥认证方法的 IPSec VPN 的配置过程。

❶ 首先，在远程办公网络的边界路由器上，定义 ISAKMP 和管理连接的 IKE。

```
Remote(config)# crypto isakmp enable        //启用IKE
Remote(config)# crypto isakmp identity address
Remote(config)# crypto isakmp policy 10     //创建标识为“100”的IKE策略
Remote(config-isakmp)# encryption aes 128 //使用des加密方式，密钥长度为128位
Remote(config-isakmp)# hash md5    //指定hash算法为MD5(其他方式如sha、rsa)
Remote(config-isakmp)# authentication pre-share//使用预共享的密码进行身份验证
Remote(config-isakmp)# group 1 //指定密钥位数，group 2安全性更高，但更耗cpu
```

```
Remote(config-isakmp)# exit
```

❷ 然后定义预共享密钥，并指定 VPN 另一端路由器的 IP 地址。

```
Remote(config)# crypto isakmp key sadness123 address 10.0.0.1 255.255.255.255
no-xauth
```

❸ 再定义需要加密流量的 ACL，例如远程用户的 IP 地址范围为 192.168.1.0/24，公司总部的 IP 地址范围是 192.168.2.0/24。

```
Remote(config)# ip access-list extended Local
Remote(config-ext-nacl)#  permit  ip  192.168.1.0  0.0.0.255  192.168.2.0
0.0.0.255
```

❹ 接着还需要定义远程连接的静态路由。

```
Remote(config)# ip route 192.168.2.0 255.255.255.0  10.0.0.1
```

❺ 设置加密转换规则。

```
Remote(config)# crypto ipsec transform-set Local esp-aes esp-md5-hmac
Remote(cfg-crypto-tran)# exit
```

❻ 创建加密映射。

```
Remote(config)# crypto map sadnessMAP 10 ipsec-isakmp
Remote(config-crypto-m)# set peer 10.0.0.1
Remote(config-crypto-m)# set transform-set Local
Remote(config-crypto-m)# match address Local
Remote(config-crypto-m)# exit
```

❼ 通过定义本地 ACL，允许或禁止哪些数据通过 VPN 送到总部网络。

```
Remote(config)# ip access-list extended local-acl
Remote(config-ext-nacl)# permit udp host 10.0.0.1 host 10.1.1.1 eq 500
Remote(config-ext-nacl)# permit esp host 10.0.0.1 host 10.1.1.1
Remote(config-ext-nacl)#  permit  ip  192.168.2.0  0.0.0.255  192.168.1.0
0.0.0.255
Remote(config-ext-nacl)# deny ip any any
Remote(config-ext-nacl)# exit
```

❽ 最后，将上述定义的本地 ACL 和 Crypto Map 应用到某个网络接口上。

```
Remote(config)# interface GigabitEthernet0/0
Remote(config-if)# ip address 10.1.1.1 255.255.255.0
Remote(config-if)# ip access-group local-acl in
Remote(config-if)# crypto map sadnessMAP
```

❾ 对总部边界路由器的配置方法与上述相似，以下是其配置过程。

```
Local(config)# crypto isakmp enable
Local(config)# crypto isakmp identity address
Local(config)# crypto isakmp policy 10
Local(config-isakmp)# encryption aes 128
Local(config-isakmp)# hash md5
Local(config-isakmp)# authentication pre-share
Local(config-isakmp)# group 1
```

```
Local(config-isakmp)# exit
Local(config)# crypto isakmp key sadness123 address 10.1.1.1 255.255.255.255
no-xauth
Local(config)# ip access-list extended Remote
Local(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Local(config-ext-nacl)# exit
Local(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
Local(config)# crypto ipsec transform-set Remote esp-aes esp-md5-hmac
Local(cfg-crypto-tran)# exit
Local(config)# crypto map sadnessMAP 10 ipsec-isakmp
Local(config-crypto-m)# set peer 10.1.1.1
Local(config-crypto-m)# set transform-set Remote
Local(config-crypto-m)# match address Remote
Local(config-crypto-m)# exit
Local(config)# ip access-list extended local-acl
Local(config-ext-nacl)# permit udp host 10.1.1.1 host 10.0.0.1 eq 500
Local(config-ext-nacl)# permit esp host 10.1.1.1 host 10.0.0.1
Local(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Local(config-ext-nacl)# deny ip any any
Local(config-ext-nacl)# exit
Local(config)# interface Ethernet0/0
Local(config-if)# ip address 10.0.0.1 255.255.255.0
Local(config-if)# ip access-group local-acl in
Local(config-if)# crypto map sadnessMAP
```

⑩ 配置完远程办公网络的边界路由器和总部边界路由器后，需要测试 VPN 连接。测试方法是，在总部边界路由器开启 debug crypto ipsec，使用扩展 ping 命令测试两个环回接口之间的流量是否被加密，由于开启了 debug 能够看到详细的 IKE 交换过程。使用 show crypto ipsec sa 命令能够看到加密数据包的流量统计以及 IPSEC 的状态。

2. 使用 CA 证书的公钥认证

对于路由器而言，使用预共享密钥将会带来一些安全性问题，当第三方使用了相同的密钥后，黑客很有可能加入到这样的 VPN 中，伪造一些数据流量。一个架构良好的公钥体系，在信任状的传递中不造成任何信息外泄，能解决很多安全问题。IPSec 与特定的公钥体系相结合，可以提供基于电子证书的认证。

假设我们使用 Microsoft CA 服务器为路由器的 IPSec 提供 CA 认证，其配置方法如下。

❶ 访问如下网站，为 CA 服务器加载 Cisco 路由器支持，如图 10-2 所示。

```
http://www.microsoft.com/china/windowsserver2003/techinfo/reskit/tools/d
efault.mspx
```

❷ 安装完成后，访问认证服务器 http://< CA ip>/certsrv/mscep/mscep.dll 记录下 challenge password(挑战密码)，如图 10-3 所示。

❸ 证书注册对时间要求很高，但由于大多数 Cisco 路由器和交换机都没有内部时钟，无法保存时间，因此必须在开机后对时间进行设置以保证证书注册的顺利完成，并且设置域名和 CA Server 的 IP 地址。

```
Remote#clock set 11:13:55 21 July 2008
Remote(config)#clock timezone GMT +8
Remote(config)#ip domain-name sadness.com
Remote(config)#ip host sadnessCA 192.168.1.100
```



图 10-2　下载 CepSetup.exe

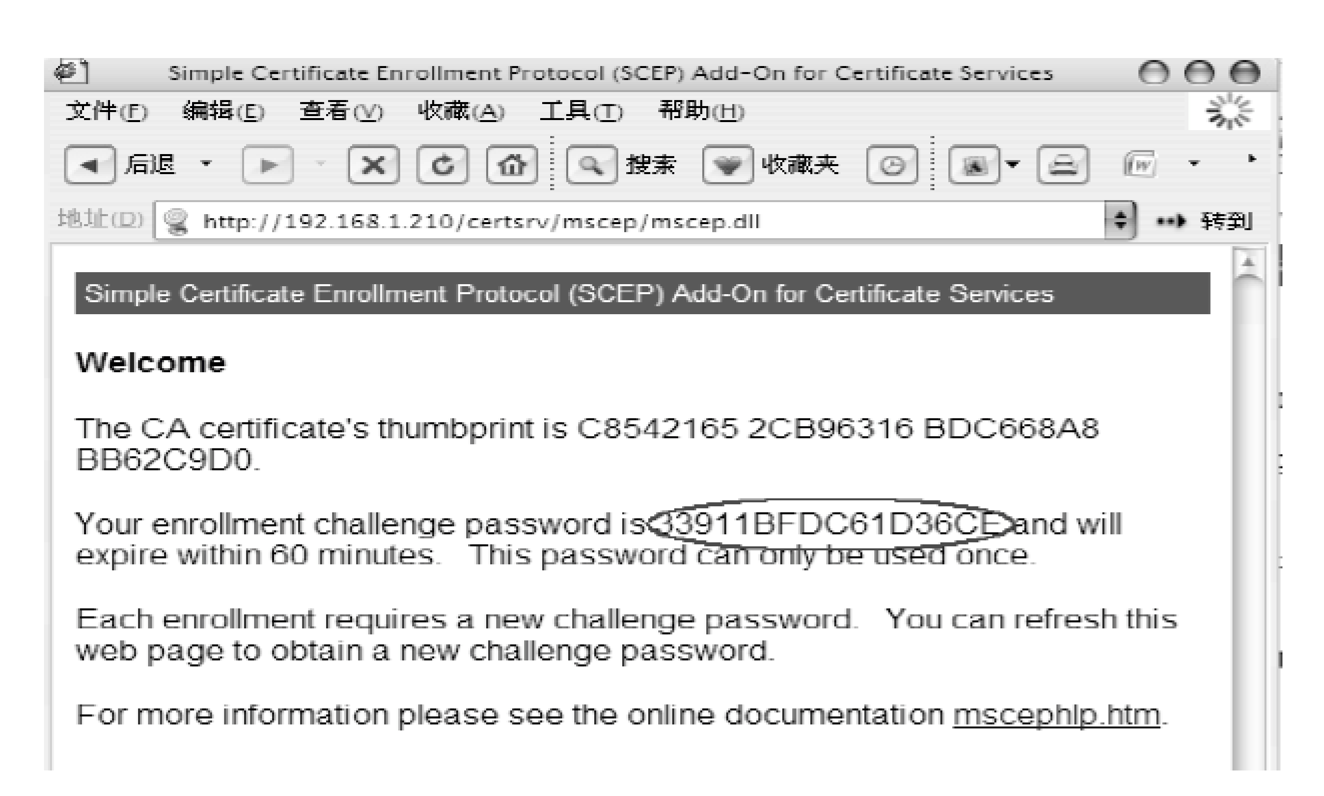


图 10-3　查询 challenge password

❹ 配置认证。

```
Remote(config)#crypto key generate rsa
Remote(config)#crypto pki trustpoint sadnessCA
Remote(ca-identity)#enrollment mode ra
Remote(ca-identity)#enrollment url http://sadnessCA/certsrv/mscep/mscep.dll
Remote(ca-identity)#exit
Remote(config)#crypto pki authenticatie sadnessCA
Remote(config)#crypto pki enroll sadnessCA
Password:           //填入第二步查询到的challenge password
Re-enter password:
```

❺ 创建 IPSec。

```
Remote(config)# crypto isakmp enable
Remote(config)# crypto isakmp identity address
Remote(config)#crypto isakmp enable
Remote(config)#crypto isakmp policy 10
Remote(config-isakmp)#authentication rsa-sig
Remote(config-isakmp)#encryption des
Remote(config-isakmp)#hash md5
Remote(config-isakmp)#group 2
```

```
Remote(config)# ip access-list extended Remote
Remote(config-ext-nacl)#  permit  ip  192.168.2.0  0.0.0.255  192.168.1.0
0.0.0.255
Remote(config-ext-nacl)# exit
Remote(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
Remote(config)# crypto ipsec transform-set Remote esp-aes esp-md5-hmac
Remote(cfg-crypto-tran)# exit
Remote(config)# crypto map sadnessMAP 10 ipsec-isakmp
Remote(config-crypto-m)# set peer 10.1.1.1
Remote(config-crypto-m)# set transform-set Remote
Remote(config-crypto-m)# match address Remote
Remote(config-crypto-m)# exit
Remote(config)# ip access-list extended Remote-acl
Remote(config-ext-nacl)# permit udp host 10.1.1.1 host 10.0.0.1 eq 500
Remote(config-ext-nacl)# permit esp host 10.1.1.1 host 10.0.0.1
Remote(config-ext-nacl)#  permit  ip  192.168.1.0  0.0.0.255  192.168.2.0
0.0.0.255
Remote(config-ext-nacl)# deny ip any any
Remote(config-ext-nacl)# exit
```

❻ 将本地 ACL 和 Crypto Map 应用到接口。

```
Remote(config-if)# ip address 10.0.0.1 255.255.255.0
Remote(config-if)# ip access-group Remote-acl in
Remote(config-if)# crypto map sadnessMAP
```

❼ 使用上一节所述的同样方法测试 VPN 连接。

10.3　拨号虚拟专网

应用实例导航：为 Sadness 公司部署员工远程接入访问

※场景呈现

Sadness 公司员工希望在自己家中通过一种简单的方式连接到公司网络以实现在家办公，因此 Jam 需要为他们建立一种方便而安全的接入方式。

※技术要领

(1)　基于 ISA Server 2004 的 VPN 服务器端配置；
(2)　VPN 客户端的配置；
(3)　基于 Cisco VPDN 的 VPN 服务器端的配置；
(4)　基于 Linux 的 VPN 服务器端的配置。

10.3.1　VPDN 概述

基于拨号虚拟专网(Virtual Private Dial-up Networks，VPDN，俗称“网中网”)是利用公共网络(如 ISDN 和 PSTN)的拨号功能及接入网来实现虚拟专用网，为企业、小型 ISP、移动

办公人员提供接入服务。VPDN 采用专用的网络加密和通信协议，可以使企业在公共 IP 网络上建立安全的虚拟专网。例如，企业分支机构、企业员工离开公司出差中可以从远程经过公共 IP 网络，通过虚拟的加密通道与企业内部的网络连接，而公共网络上的客户则无法穿过虚拟通道访问该企业的内部网络。VPDN 能够充分利用现有的网络资源，提供经济、灵活的联网方式，为客户节省设备、人员和管理所需要的投资，降低用户的费用，应用非常广泛。

VPDN 主要由网络接入服务器(NAS)、用户端设备(CPE)和管理工具组成。其中 NAS 由大型 ISP 或电信部门提供，其作用是作为 VPDN 的接入服务提供广域网接口，负责与 PSTN、ISDN 的连接，并支持各种 LAN 的协议、安全管理和认证、隧道及相关技术；CPE 是 VPDN 的用户端设备，位于用户总部，根据网络功能的不同可以是由 NAS、路由器或防火墙等提供相关的设备来担任；VPDN 管理工具对 VPDN 设备和用户进行管理。

VPDN 的协议可以基于第二层隧道协议，如 PPTP、L2F、L2TP，也可基于第三层隧道协议，如 IPSec。一般情况下，VPDN 所用的协议为 L2TP 协议。

VPDN 的协议工作原理是，当 VPN 用户拨号时，网络接入服务器(NAS)与公司的企业网关之间直接建立一个隧道。此后，各种网络协议(如 TCP、IP、IPX 等协议)产生的用户数据经过一系列封装，通过隧道传递到企业网关，再进行解包，数据才传递到企业内部。

VPDN 可以用一台 VPND 路由器或网关担任，当然也可以用安装多块网卡的 Windows 或 Linux 主机来担任。

10.3.2 配置基于 ISA Server 2004 的 VPN

ISA Server 2004 防火墙可以配置为 VPN 服务器或者 VPN 网关。VPN 服务器组件允许接受远程 VPN 客户端的访问请求，在成功建立 VPN 连接后，VPN 客户可以成为一个受保护的网络成员。ISA Server 2004 的 VPN 网关允许在 Internet 上连接一个完整的网络。

1. 配置 VPN 服务器

下面简要介绍一下基于 ISA Server 2004 的 VPN 的配置过程。

❶ 依次单击【开始】→【程序】→Microsoft ISA Server→【ISA 服务器管理】命令。在打开的 ISA 服务器管理控制台窗口中，依次选择【阵列】→Sadness ISA→【虚拟专用网络(VPN)】结点，如图 10-4 所示。

❷ 选择右侧【任务】选项卡中的【定义地址分配】链接，添加一个静态地址池用于拨入用户使用的 IP，如图 10-5 所示。

❸ 单击图 10-4 右侧【启用 VPN 客户端访问】链接并应用配置，完成后该链接会变为【禁用 VPN 客户端访问】链接，如图 10-6 所示。

❹ 单击【配置 VPN 客户端访问】链接，在打开的对话框中设置最大 VPN 客户端数量，并在【协议】选项卡中选中【启用 L2TP/IPSec】复选框以获得较高的安全性，如图 10-7 所示。



图 10-4　配置 VPN

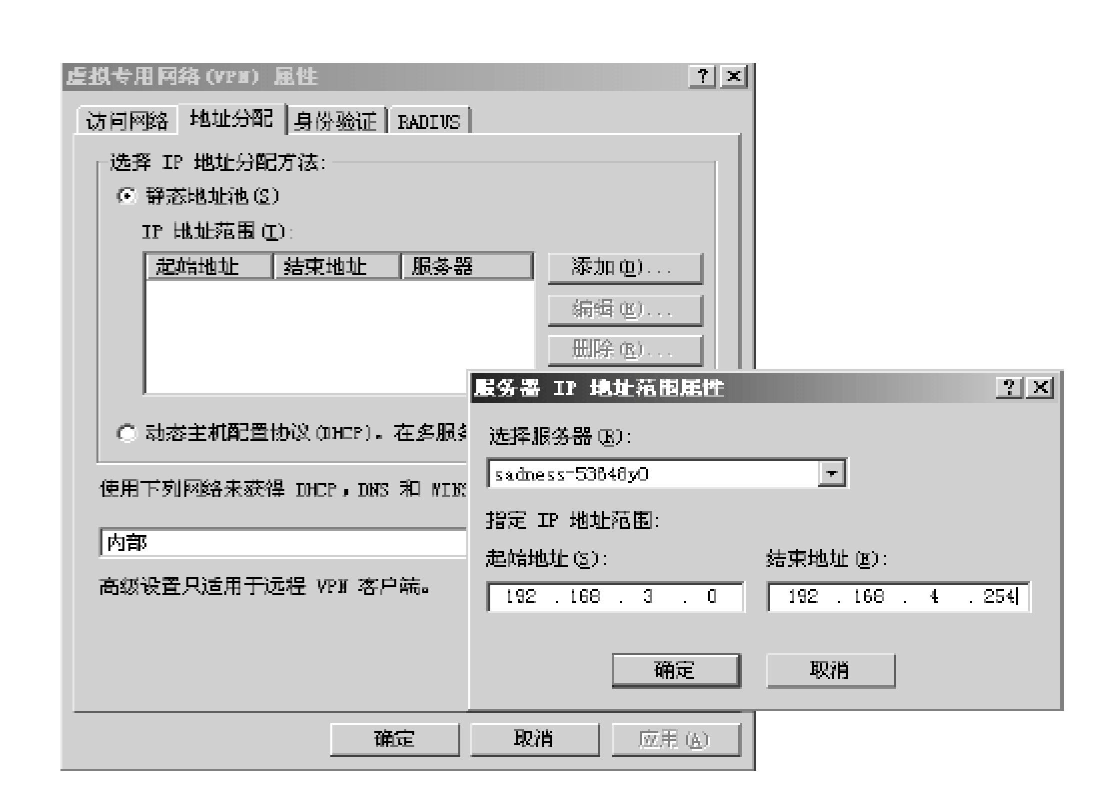


图 10-5　添加静态地址池

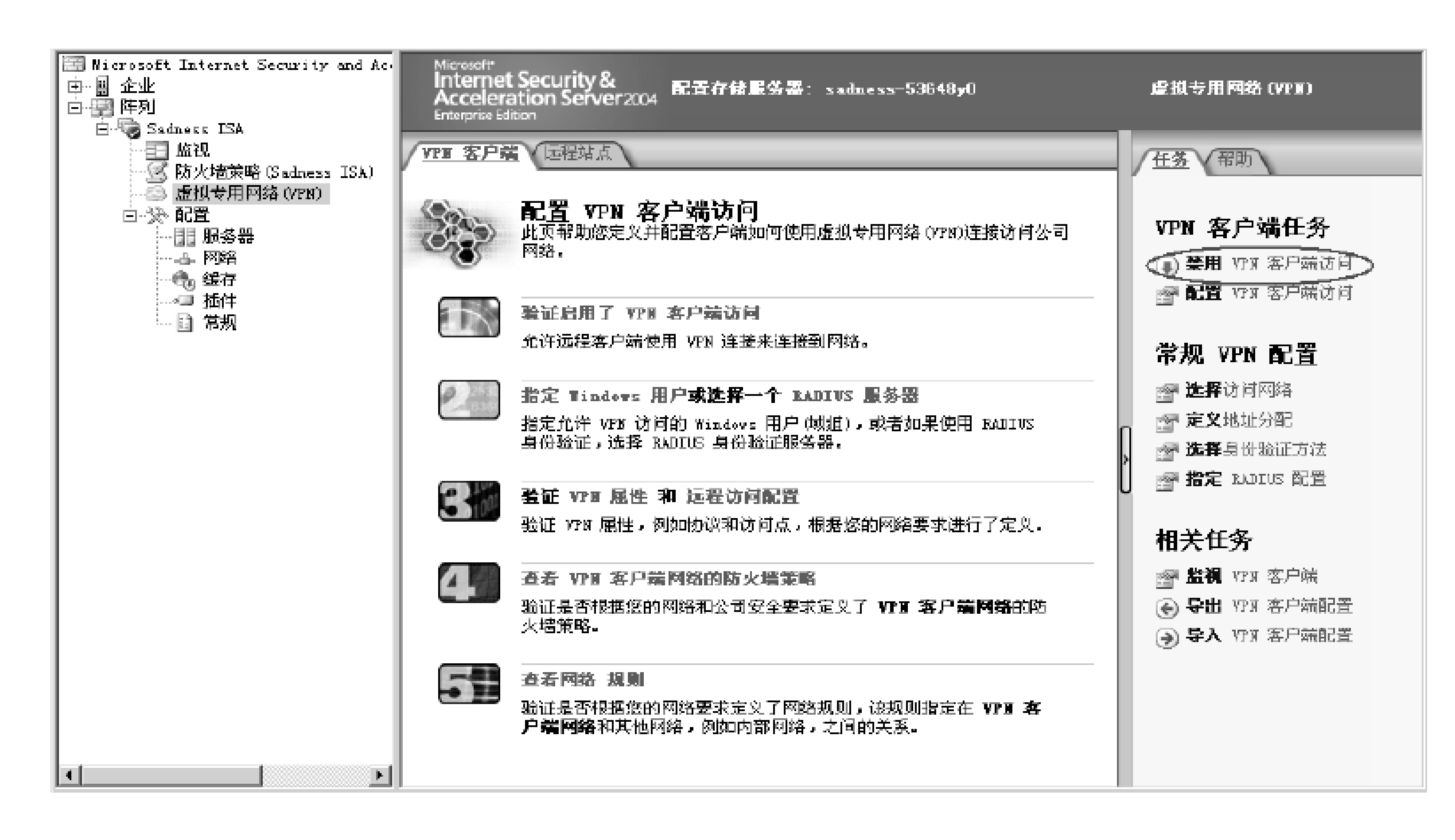


图 10-6　启用 VPN 客户端访问

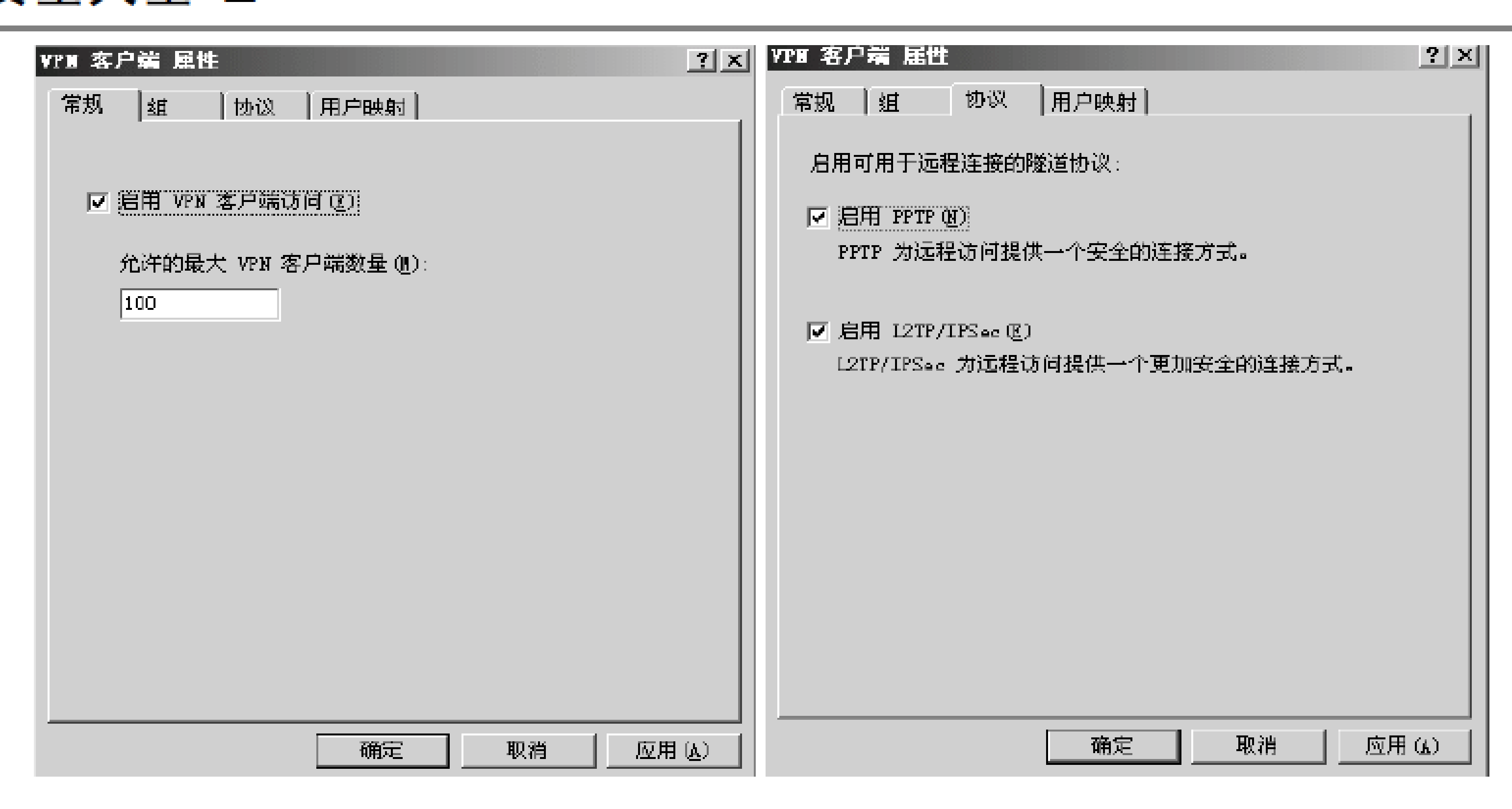


图 10-7　配置 VPN 客户端访问

❺ 新建一条访问规则，使得 VPN 和内部网络可以互相访问，如图 10-8 所示。



图 10-8　配置 VPN 访问规则

❻ 如果需要使用 RADIUS 服务器进行身份验证，则单击【指定 RADIUS 配置】链接。在打开的对话框中，选中【使用 RADIUS 进行身份验证】和【使用 RADIUS 记账】复选框，并单击【RADIUS 服务器】按钮来添加 RADIUS 服务器，如图 10-9 所示。

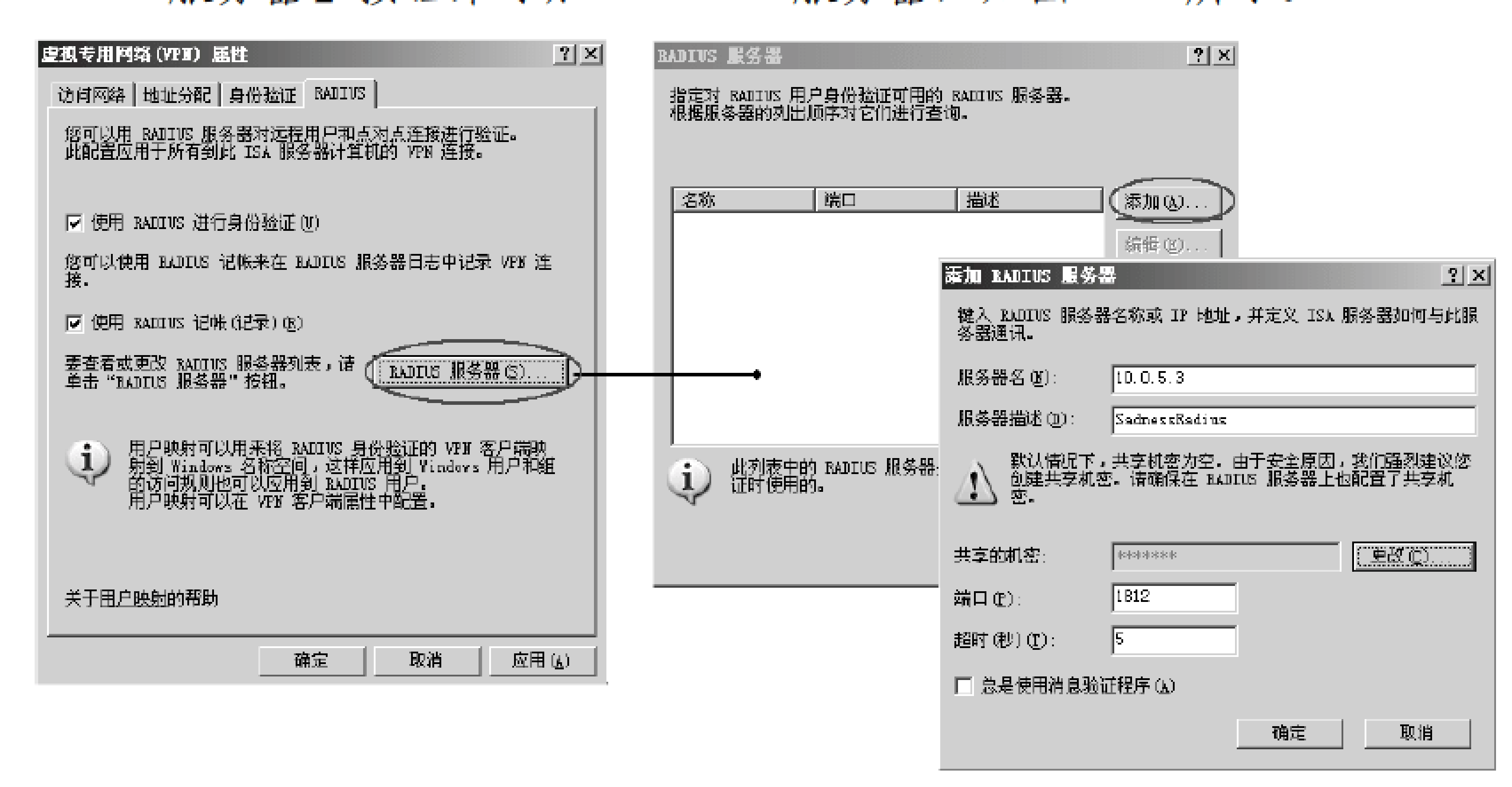


图 10-9　添加 RADIUS 服务器

❼ 如果未使用 RADIUS 认证，则需要打开【Active Directory 用户和计算机】控制台窗口，在目录树中选择 Sadness.com→Users 结点，在右侧窗格中选择需要远程接入的用户，然后右击，在弹出的快捷菜单中选择【属性】命令。在用户属性对话框中，切换到【拨入】选项卡，选中【允许访问】单选按钮，如图 10-10 所示。

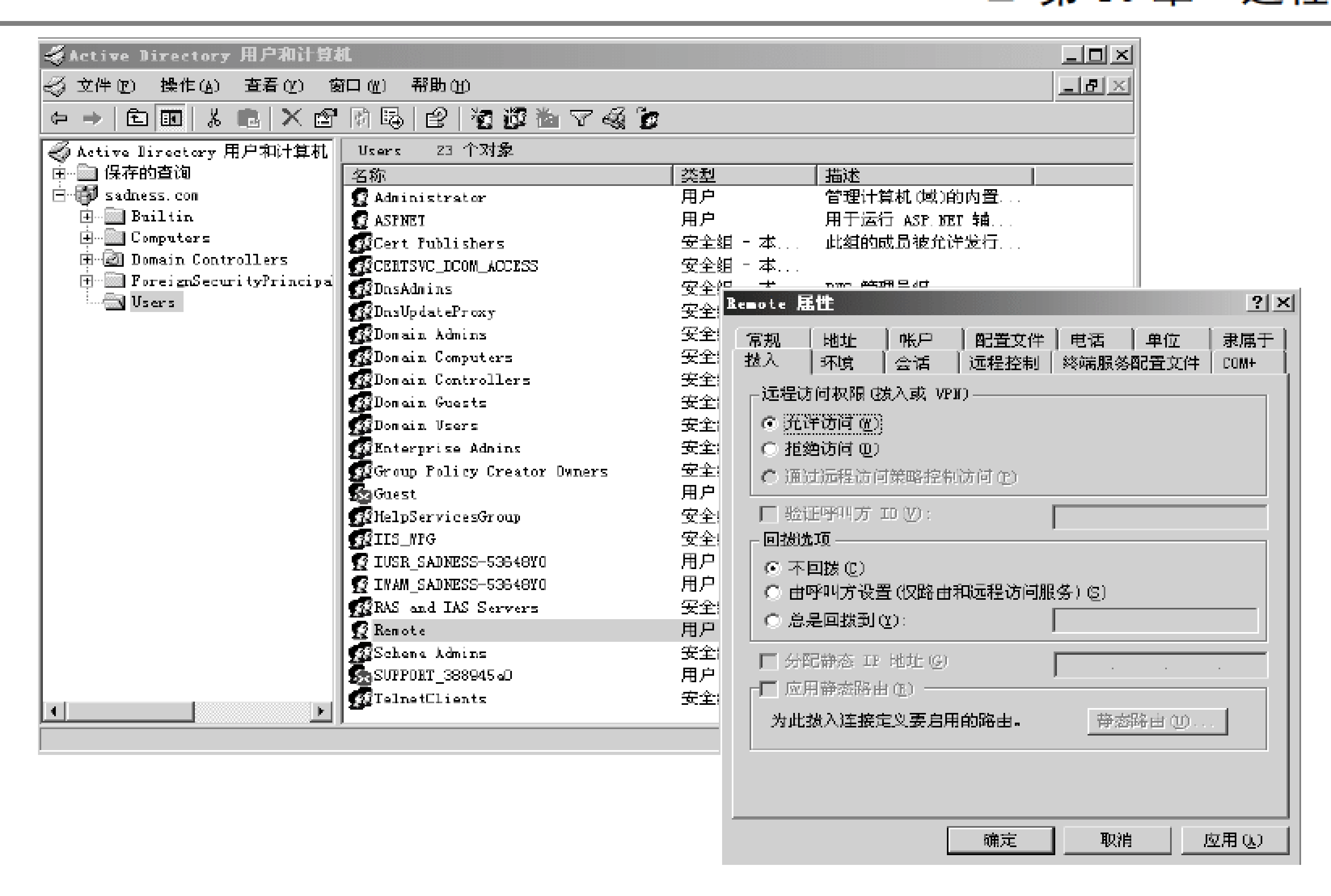


图 10-10　配置远程访问权限

2. VPN 客户端的设置与测试

当 VPN 服务器架设好，并赋予用户远程访问的权限后，就可以从 VPN 客户机连接到 VPN 服务器了。在连接之前，还要创建 VPN 拨号连接，操作步骤如下。

❶ 完成服务器端配置后，在客户端中依次选择【控制面板】→【网络连接】→【新建连接向导】图标，在新建连接向导页中单击【下一步】按钮；在【网络连接类型】向导页选中【连接到我的工作场所的网络】单选按钮，单击【下一步】按钮；在【网络连接】向导页，选中【虚拟专用网络连接】单选按钮，然后单击【下一步】按钮 ，如图 10-11 所示。



图 10-11　在客户端创建 VPN 连接

❷ 在【连接名】向导页，输入连接的名称，例如“VPDN to Sadness”，然后单击【下一步】按钮；在【VPN 服务器选择】向导页，输入 ISA 服务器的外部 IP 地址或公司 VPDN 服务器的域名，单击【下一步】按钮，如图 10-12 所示。



图 10-12　设置连接名称和 VPN 服务器

❸ 完成 VPDN 客户端配置后，单击 VPDN to Sadness 图标，开始连接 VPN，在对话框中输入用户名和密码，然后单击【连接】按钮，如图 10-13 所示。



图 10-13　连接到 VPDN 服务器端

❹ 系统将开始链接，完成在网络上注册计算机后，Windows 右下角会显示“VPDN to Sadnesss 现在已连接”提示信息，这样就完成了基于 ISA Server 2004 的 VPDN 配置，如图 10-14 所示。

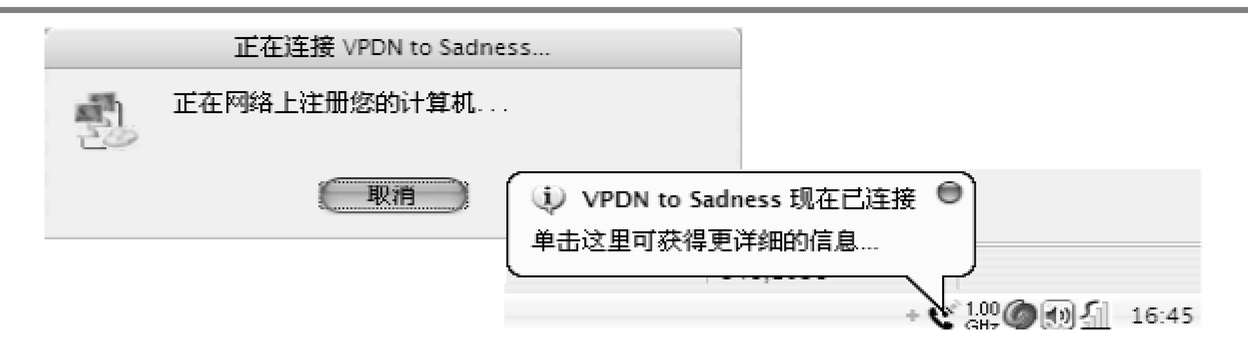


图 10-14　完成客户端连接

❺ 在客户端，使用 ipconfig 命令查看获取的 IP 地址等信息，显示连接已经建立。

```
C:/> ipconfig
PPP adapter VPDN to Sadness:
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . .  : WAN (PPP/SLIP) Interface
Physical Address. . . . . . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . ..... . : 192.168.3.114
Subnet Mask . . . . . . . . . . . : 255.255.255.255
Default Gateway . . . . . . . . : 192.168.3.114
DNS Servers . . . . . . . . . . . . : 192.168.10.3
                        192.168.10.4
```

10.3.3　使用 ASA 配置 VPN

由于 Cisco ASA (Adaptive Security Appliance，适应性安全产品)是一种常见的 UTM(Unified Threat Management，统一威胁管理)设备，在防火墙的基础上集成了 IPS、防病毒网关等众多功能，同时还集成了 VPN 的功能，通过与 Cisco VPN Client 配合实现了 VPDN 服务。下面简要地介绍一下通过 ADSM(自适应安全设备管理器)配置 ASA 的 VPDN 过程。

❶ 启动 ADSM，单击 Wizards→IPSec VPN Wizard 命令，启动 IPSec VPN 配置向导，如图 10-15 所示。

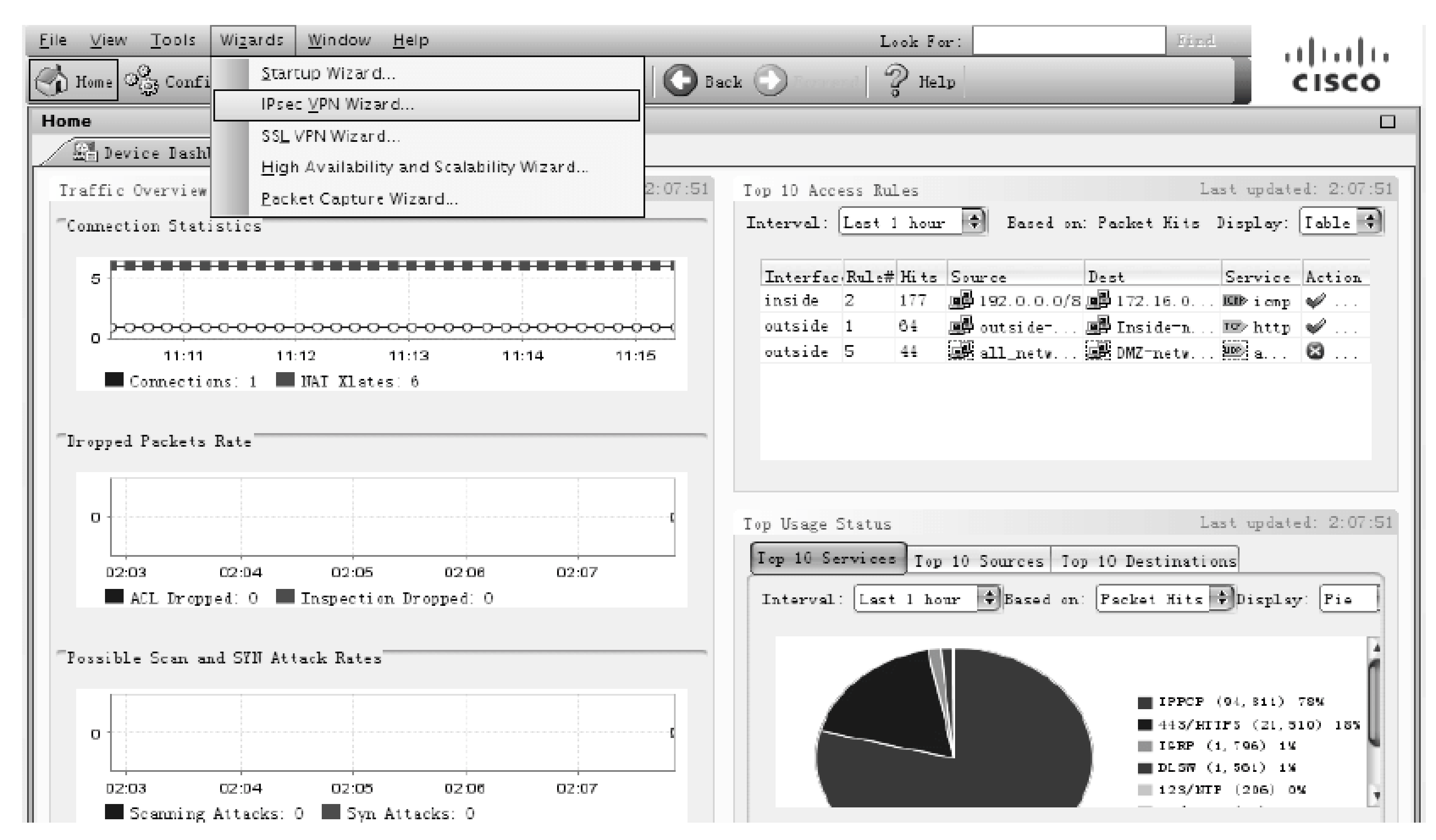


图 10-15　启动 VPN 配置向导

❷ 在 VPN 配置向导的第 1 步中，选中 Remote Access 单选按钮，将 VPN Tunnel Interface 下拉列表框设置为外部(outside)接口，然后单击 Next 按钮。第 VPN 配置向导的第 2 步中，选择 VPN 客户端模式，可以选择 Cisco VPN Client 或者微软 Windows 客户端，然后单击 Next 按钮，如图 10-16 所示。

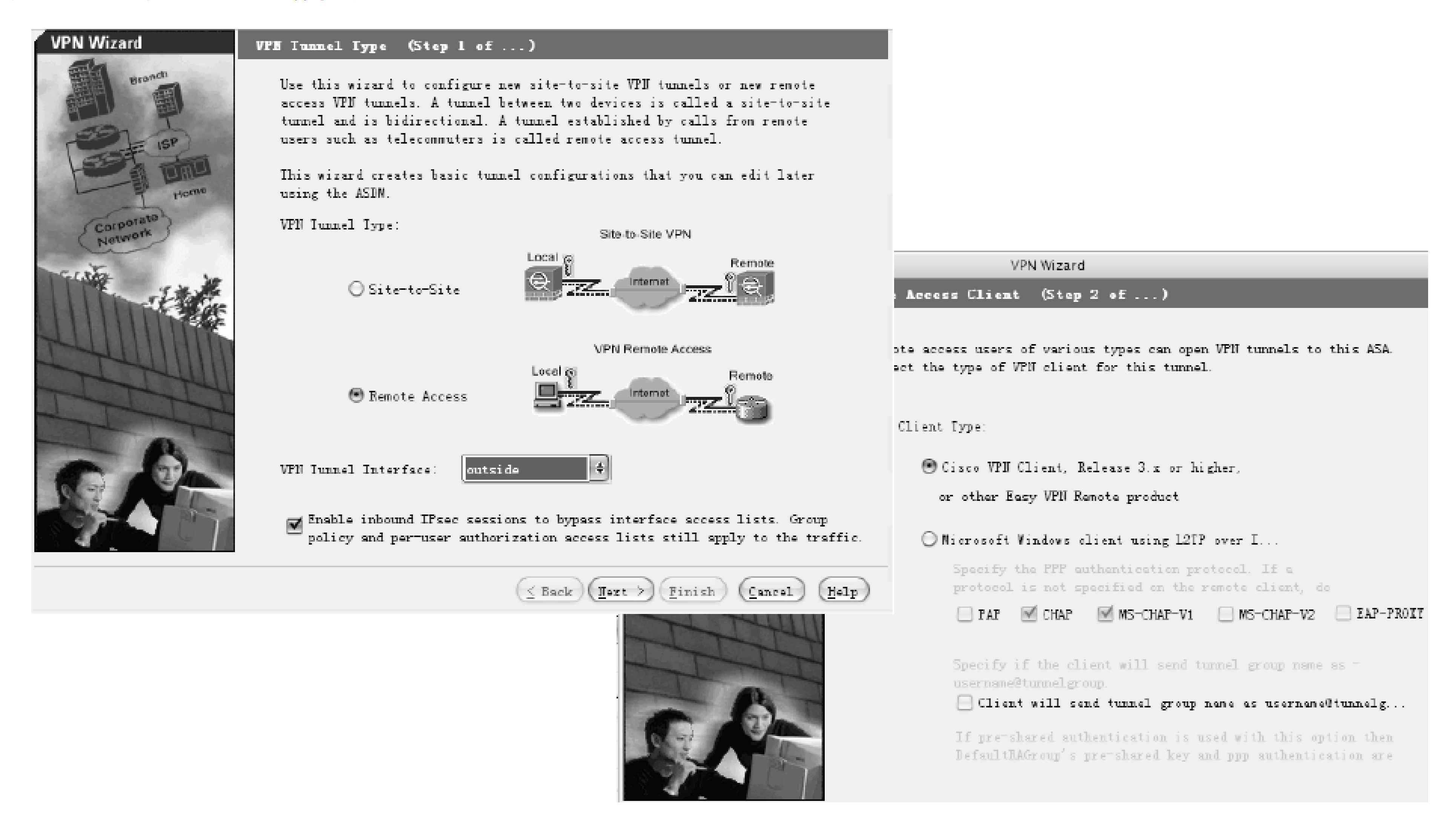


图 10-16　选择 VPN 模式及客户端

❸ 在 VPN 配置向导的第 3 步中，选择 VPN 的认证模式，可以选择 Pre-shared key 模式，也可以使用微软的 CA 认证方式，如图 10-17 所示。

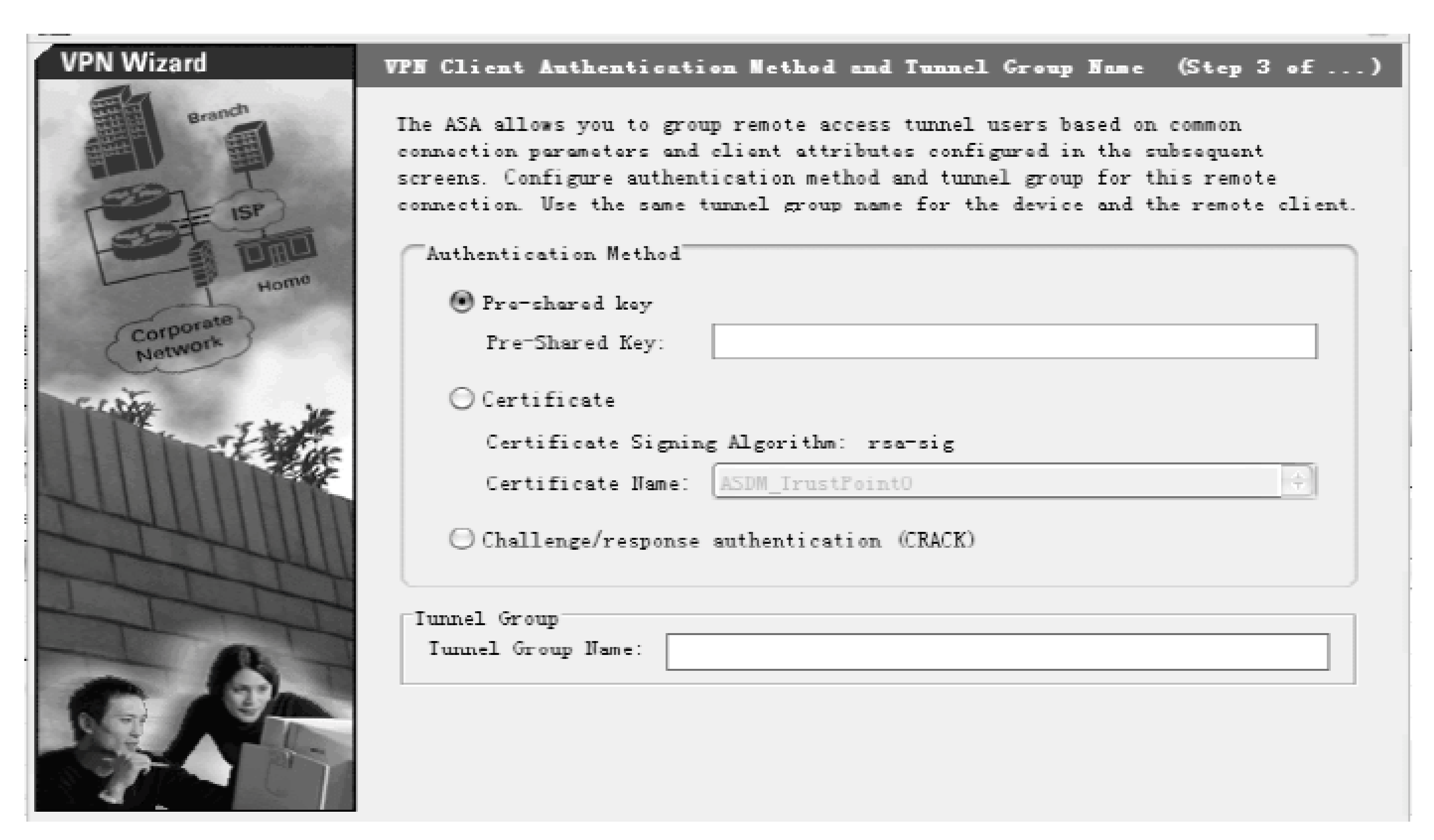


图 10-17　选择 VPN 认证模式

❹ 如果需要使用基于 CA 的认证方式，可依次单击 Remote Access VPN →Certificate Management →IdentityCertificates 结点，再单击 Add 按钮进行添加 ，如图 10-18 所示。

❺ 在 Add Identity Certificate 对话框中，单击 Advanced 按钮，按照本章前述的方式配置 Enrollment URL 及 Challenge Password，如图 10-19 所示。

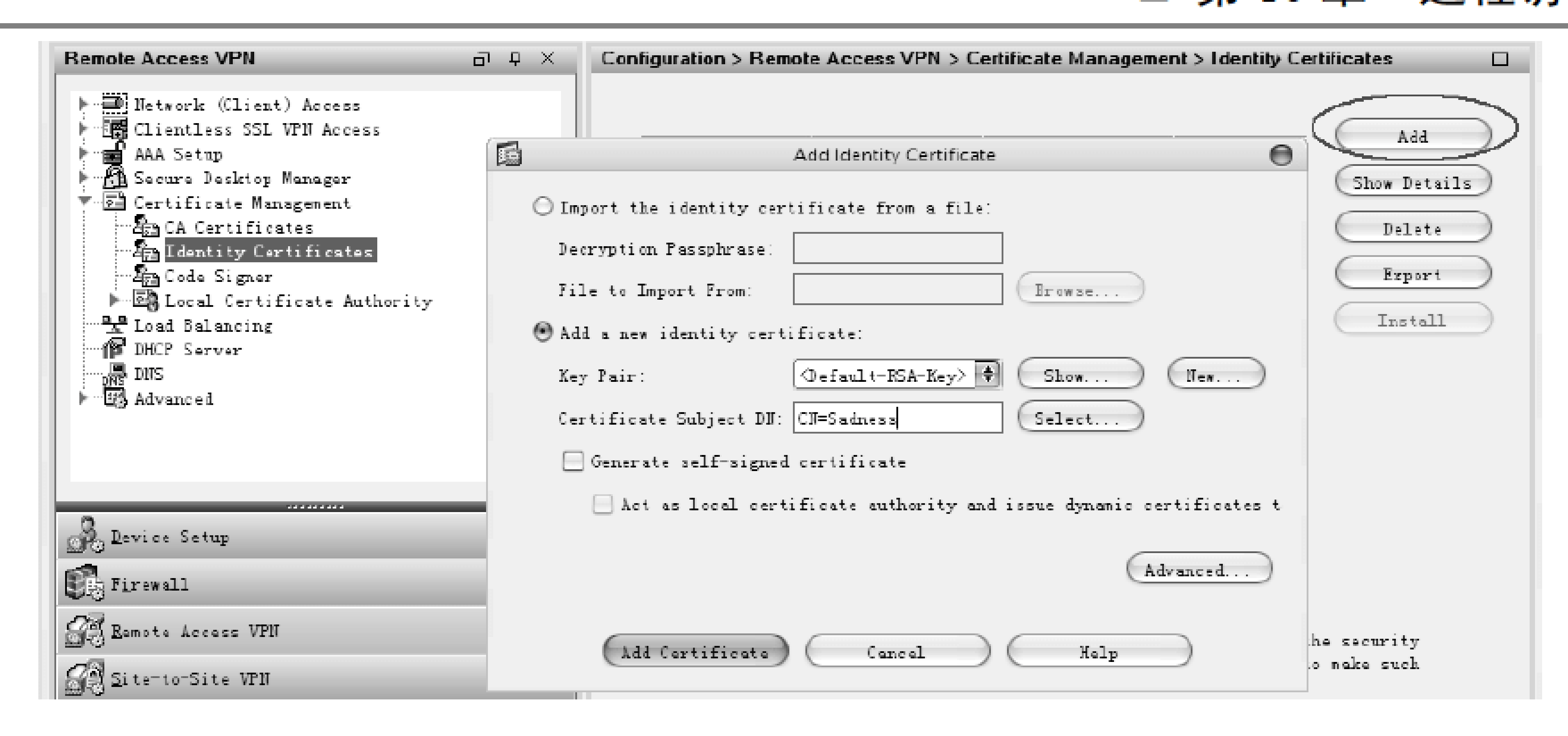


图 10-18　添加 CA 认证方式



图 10-19　配置 CA 认证

❻ 在 VPN 配置向导的第 3 步中，设置 VPN 认证模式。选择相应的证书名称(Certificate Name)，并定义隧道组名称(Tunnel Group Name)，如图 10-20 所示。

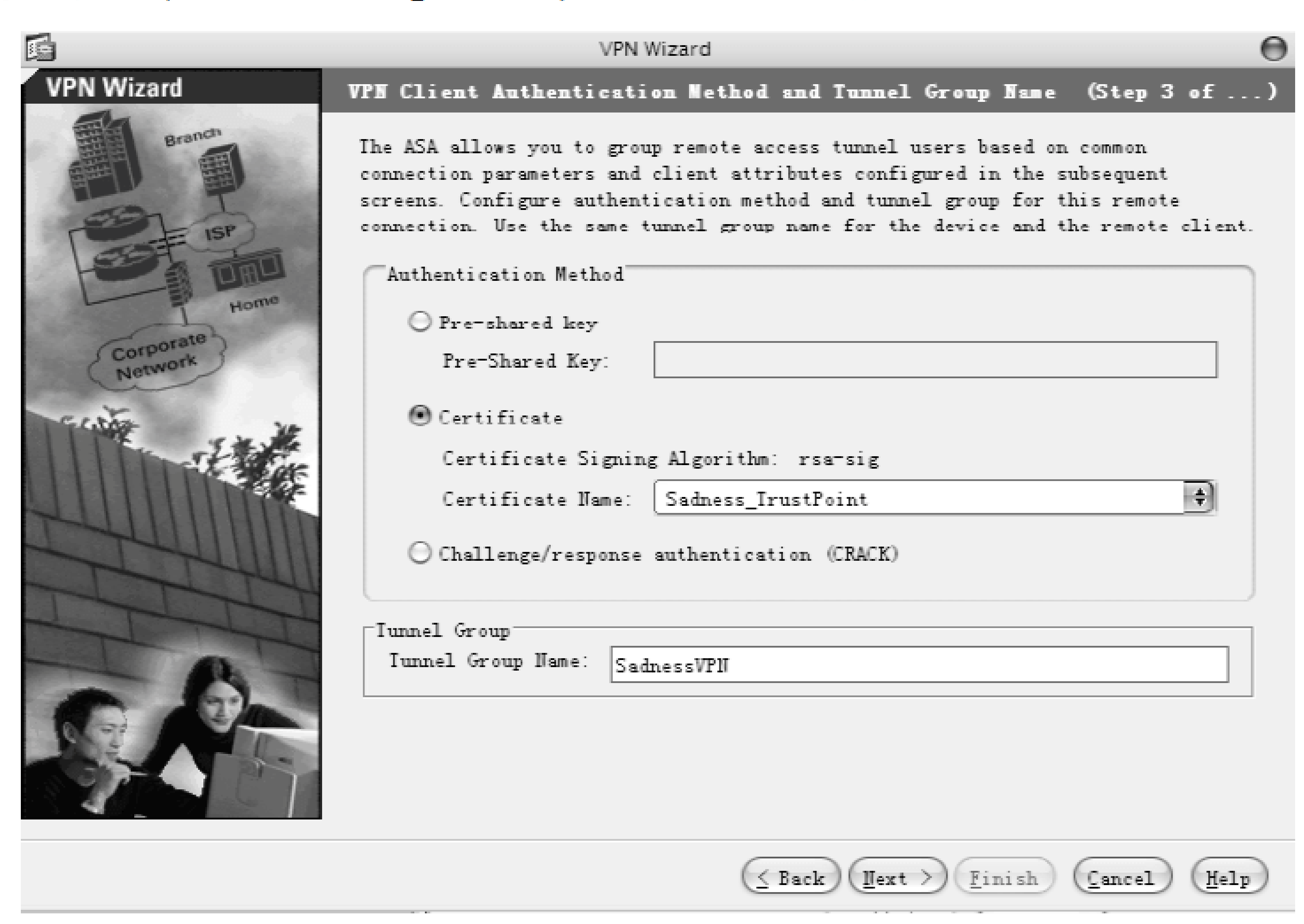


图 10-20　配置 VPN 认证模式

❼ 在 VPN 配置向导的第 4 步中，设置客户信息所使用的认证方式，可以选择 ASA 使用本地认证，也可以使用外置的 RADIUS 服务器进行认证。如果需要 RADIUS 认证，选中 Authenticate using an AAA Server Group 单选按钮，并单击 New 按钮添加 RADIUS 服务器，如图 10-21 所示。

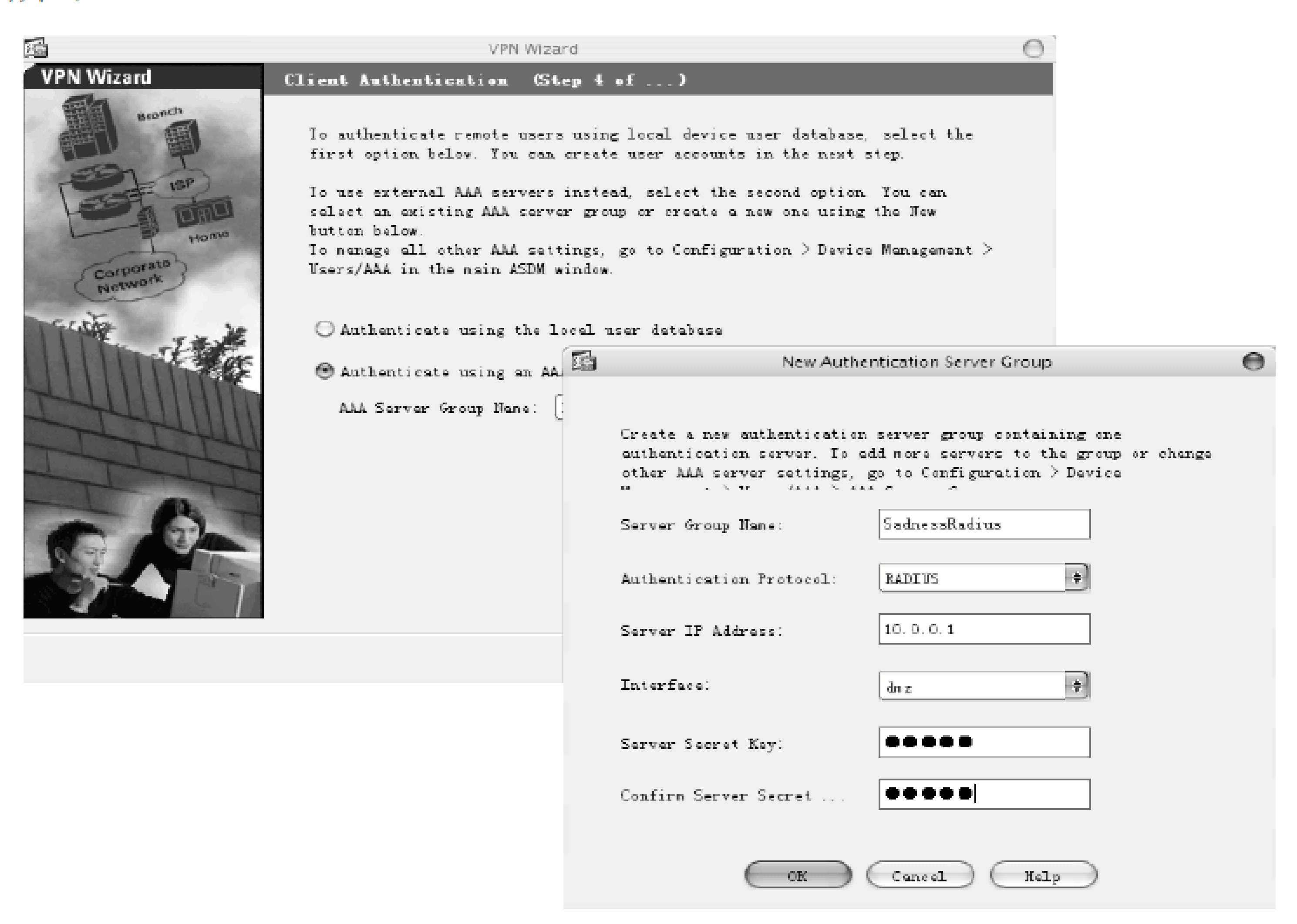


图 10-21　配置 VPN 客户端认证

❽ 在 VPN 配置向导的第 5 步中，为 VPN 客户配置静态地址池，如图 10-22 所示。



图 10-22　配置静态地址池

❾ 在 VPN 配置向导的第 6 步中，为 VPN 客户端配置 DNS 服务器、WINS 服务器和默认域名，如图 10-23 所示。

❿ 在 VPN 配置向导的第 7 步和第 8 步中，选择 IKE 规则和 IPSec 加密及认证方式，一般选择加密方式为 3DES、认证方式为 SHA，如图 10-24 所示。

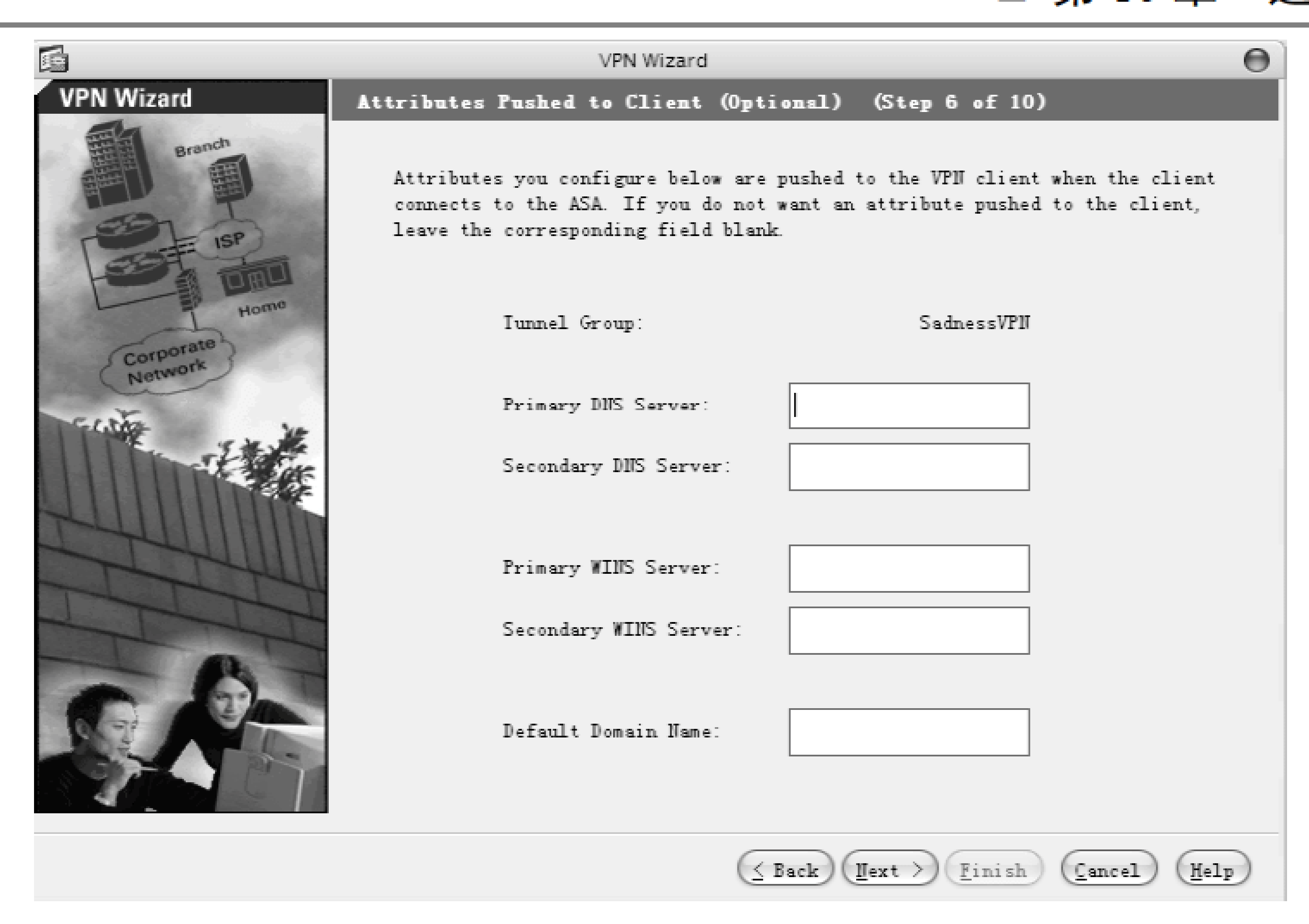


图 10-23　配置 DNS 服务器、WINS 服务器及默认域名



图 10-24　配置 IKE 规则和 IPSec 加密及认证方式

⓫ 在 VPN 配置向导的第 9 步中，配置 NAT 例外或 Split Tunnel，如图 10-25 所示。该步为可选配置。

⓬ 在 VPN 配置向导完成后，将显示总结(Summary)页面，单击 Finished 按钮确认上述配置。

⓭ 在第❷步客户端配置中，如果选择 Windows 客户端，可以按照 10.3.2 所述的方法进行配置，如果选择 Cisco VPN Client，则依次 Certificate →Enroll 按钮，按照前述方式配置 CA URLs、CA Domain 和 Challenge Password，如图 10-26 所示。

⓮ 在连接时，选择该认证方式为 Certificate Authentication 即可，如图 10-27 所示。

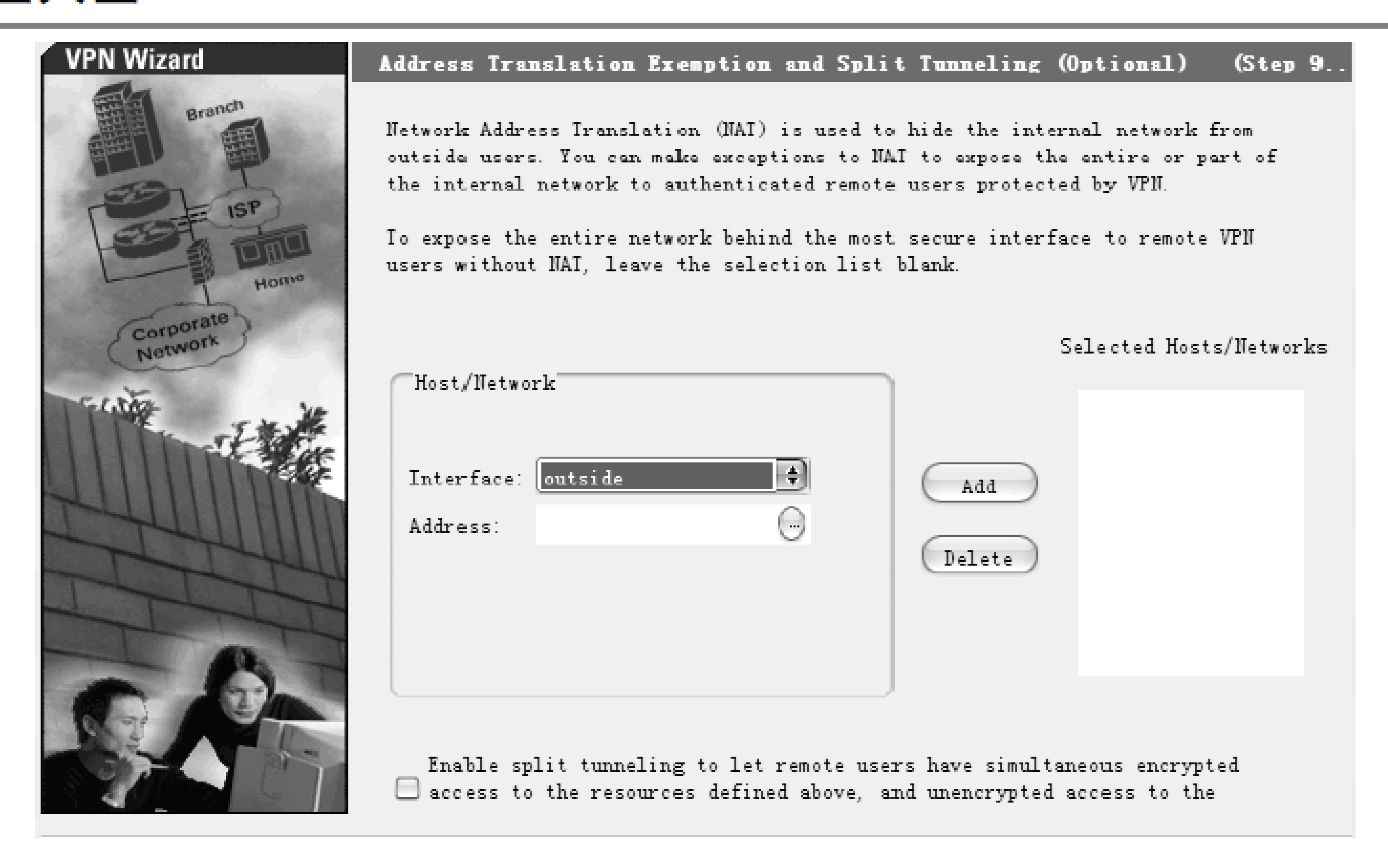


图 10-25　配置 IPSec 加密认证方式

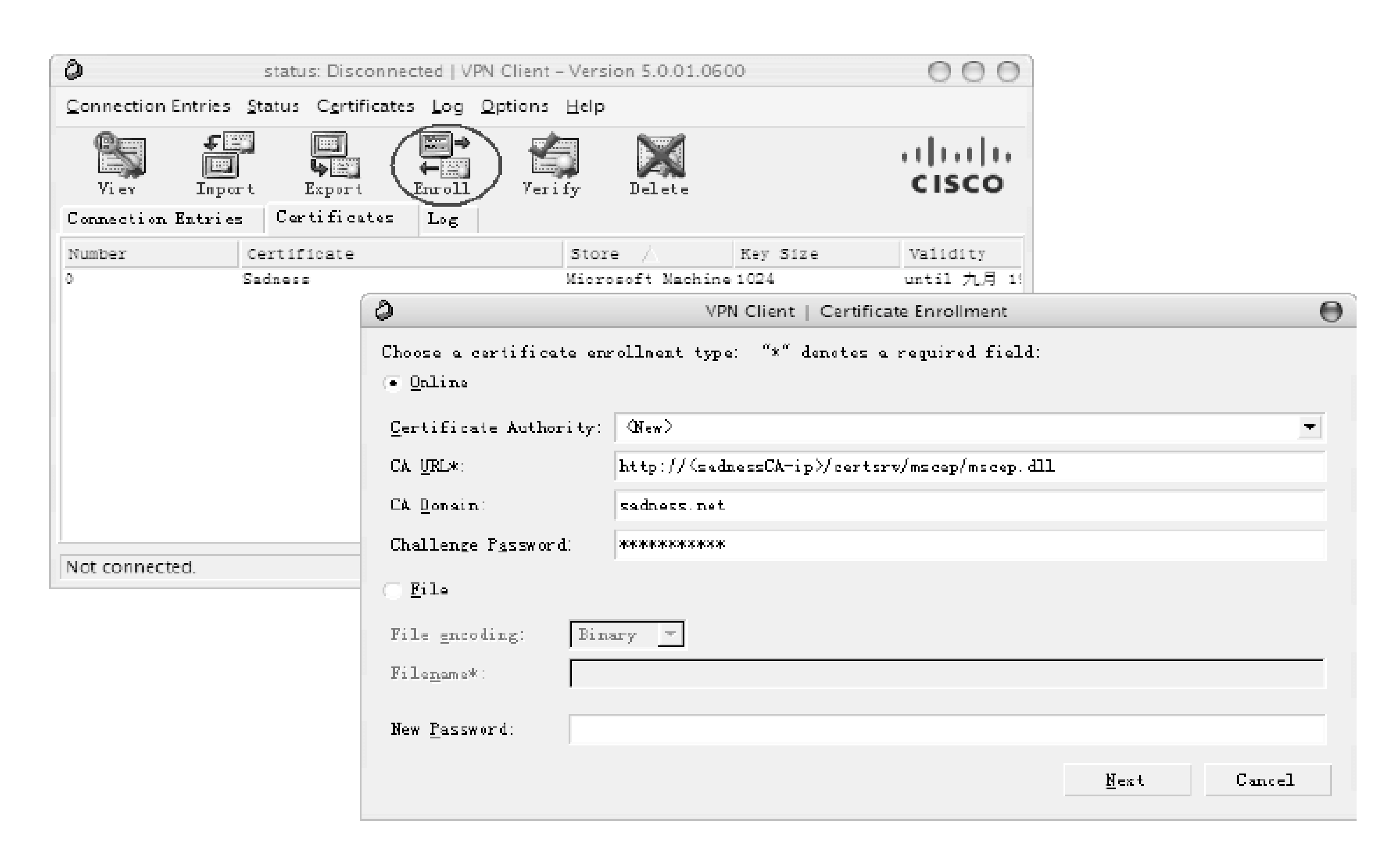


图 10-26　在 Cisco VPN 客户端配置 CA 认证

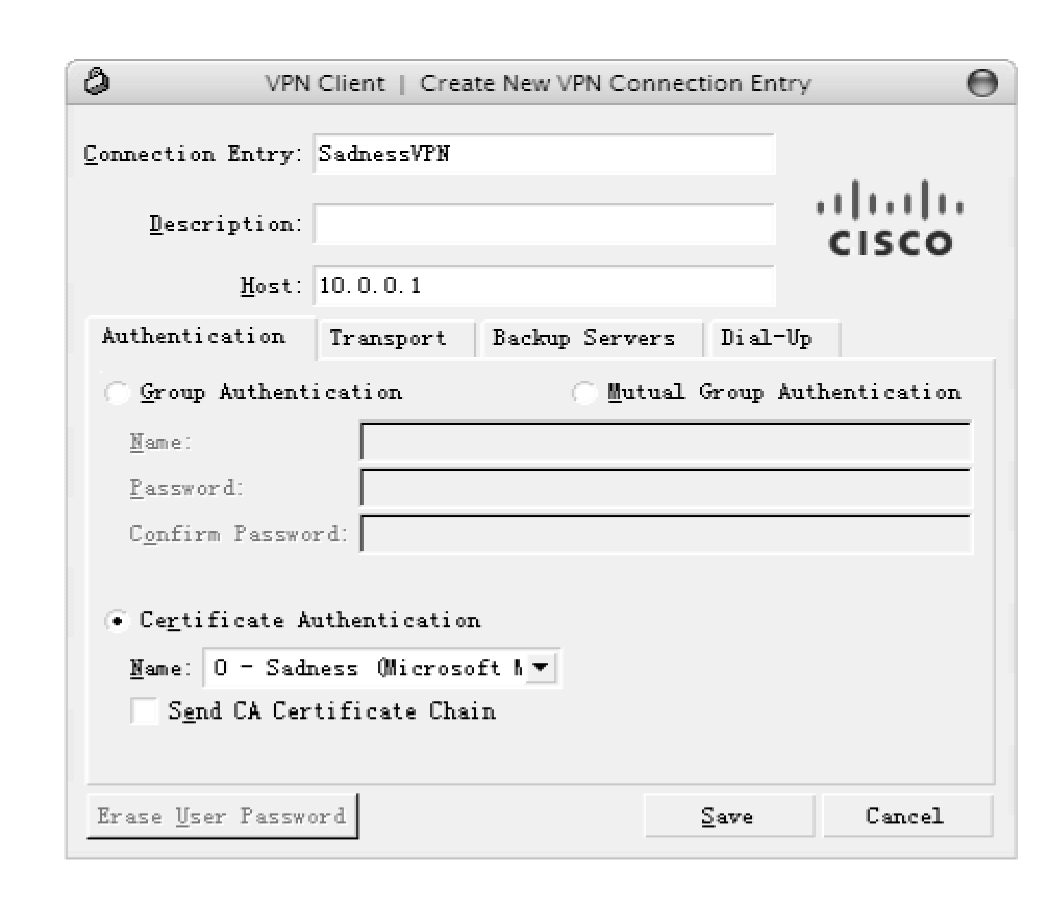


图 10-27　选择认证方式



10.3.4　配置 Linux VPN

应用实例导航：基于多 ISP 的加速 VPN 访问

※场景呈现

Sadness 公司的员工抱怨说 VPN 连接太慢，希望公司能够使用基于中国电信和中国网通的双线接入 VPN。Jam 刚好有一台做 IDS 测试的 Linux 服务器因为新购置 ASA 设备而闲置，他希望能够通过这台 Linux 配置双线 VPDN 接入中国电信和中国网通的两个 ISP 线路，如图 10-28 所示。

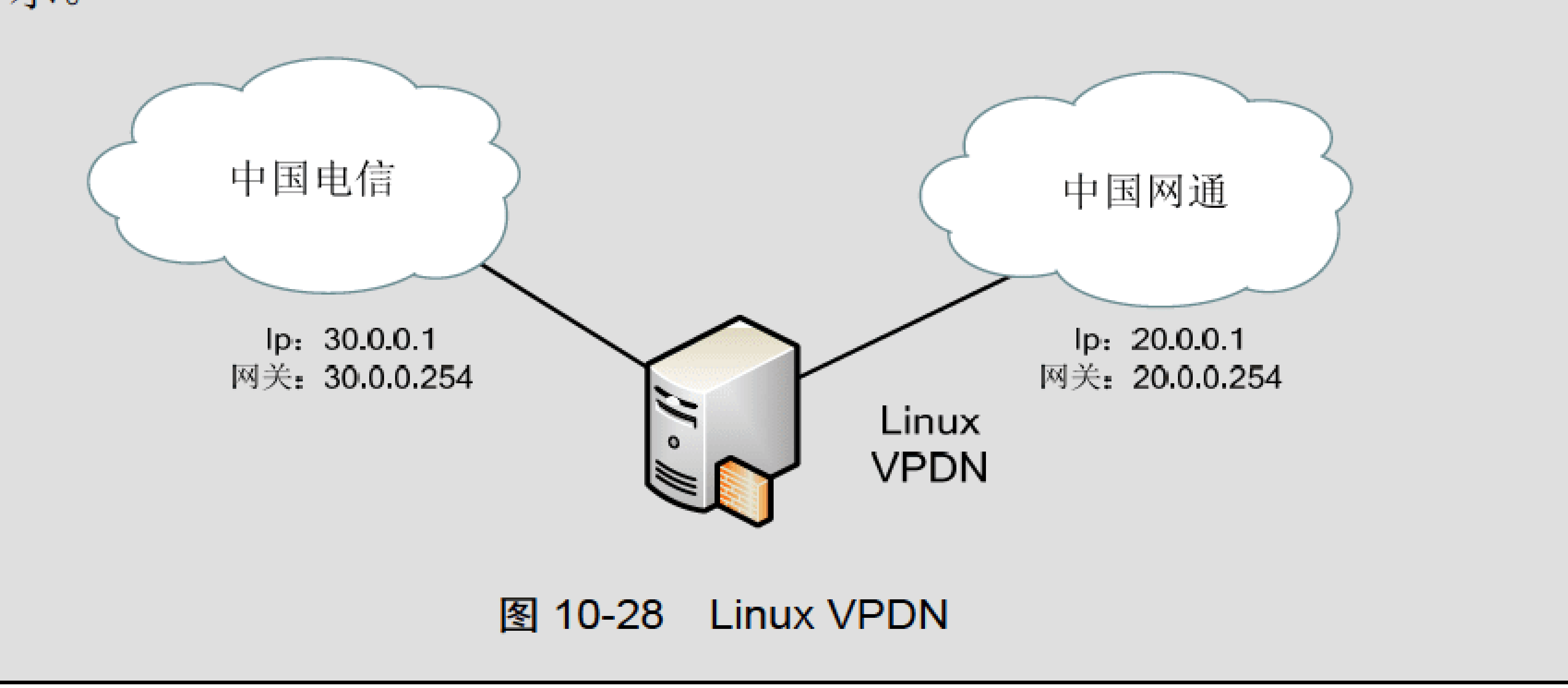


图 10-28　Linux VPDN

对于一些刚刚起步的小型企业而言，使用基于 Linux 的 VPN 服务器是一个很好的选择。下面简要介绍一下 Linux VPN 的配置过程。

❶ 根据网络连接情况配置路由表。在本例中，将电信地址段指向 30.0.0.254，其他地址指向网通的网关 30.0.0.254。

```
202.101.192.0/24 via 30.0.0.254 dev eth0  metric 10
202.113.0.0/16 via 30.0.0.254 dev eth0  metric 10
59.76.0.0/16 via 30.0.0.254 dev eth0  metric 10
                    via 30.0.0.254 dev eth0 metric 10       //电信地址段
169.254.0.0/16 dev eth1  scope link
default via 20.0.0.1 dev eth1  metric 20
```

❷ 为 VPN 地址段配置 NAT 访问规则。

```
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o eth0 -j SNAT --to-source
30.0.0.1
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o eth1 -j SNAT --to-source
20.0.0.1
```

❸ 打开网卡的数据包转发功能。

```
echo 1 >/proc/sys/net/ipv4/conf/all/forwarding
```

❹ 从 Internet 上下载并安装动态内核模块，支持软件包 DKMS、PPP 内核模块、内核

MPPE(Microsoft Point to Point Encryption，微软点对点加密)补丁、PPTP VPN 模块等软件。

5 修改 pptpd 守护进程的配置文件/etc/pptpd.conf，在该文件中添加如下两行，确定本地 VPN 服务器的 IP 地址和客户端登录后分配的 IP 地址范围。

```
localip 192.168.100.1              #本地VPN服务器的IP
remoteip 192.168.100.10-250        #分配给客户机的地址池
```

6 修改/etc/ppp/options.pptpd 文件，在该文件中添加如下内容。

```
#拒绝chap身份验证
refuse-chap
#拒绝mschap身份验证
refuse-mschap
#采用mschap-v2身份验证方式
require-mschap-v2
#注意在采用mschap-v2身份验证方式时要使用MPPE进行加密
require-mppe-128
#给客户户端分配DNS地址和WINS服务器地址
ms-dns 10.0.0.5
#启动ARP代理
Proxyarp
```

7 如果使用本地客户信息认证，需要在/etc/ppp/chap-secrets 文件中添加用户。在该文件中主要设置 4 项内容：用户名、服务、密码和分配给用户的 IP 地址，其中用户名、密码、分配给用户的 IP 地址要用双引号括起来，服务一般是“pptpd”或者设置成“*”号来表示自动识别服务器。可以指定分配给用户的 IP 地址，如果不需要做特别限制，可以将其设置为“*”号分配给用户的 IP 地址。

```
#client               server       secret       IP addresses
"jam@ sadness.com"    pptpd     "123456"      "*"
```

8 为了方便用户使用，使用一个域名代替两个网关的 IP 地址。例如在本例中，可以修改 Sadness 公司的 DNS 服务器，使 30.0.0.1、20.0.0.1 两个 IP 地址的域名都设置为 vpdn.sadness.com。

9 按照 10.3.2 所述的方法，配置 VPN 客户端并测试连接。

10.4 配置 SSL VPN

应用实例导航：为 Sadness 公司部署 Web 接入 VPN

※场景呈现

Sadness 公司总裁 Jeffy 先生希望能够在任何公众场合方便地连接到公司网络，而 VPN 需要配置客户端，比较麻烦。某次在 Jeffy 先生在机场候机时，销售部门负责人打来电话，希望 Jeffy 先生确认公司标底，Jeffy 在机场附近的公共电脑上网接收了邮件，并进行了确认。但稍后一位特殊的人物接触到 Jeffy 所使用的电脑，在那台计算机看到了标书，并转送给了竞争对手。事情发生后，Jeffy 迫切希望 Jam 能够继续提高公司的 VPN 服务。

为此，Jam 提出了使用 SSL VPN 配置方式，这种基于 Web 的方式无须使用客户端配置，并且本地存放内容均进行了加密，是一种非常安全的解决方案。某些厂商也把这种方案称为 Web VPN。

※技术要领

(1)　配置 SSL VPN；
(2)　设置 RADIUS 服务器的属性。

1. 配置 Web VPN

ADSM 内置有 Web VPN 功能，可以通过配置向导来完成 Web VPN 配置，其过程大致如下。

❶ 启动 ADSM，单击 Wizards→SSL VPN Wizard 命令，启动 SSL VPN 配置向导，如图 10-29 所示。

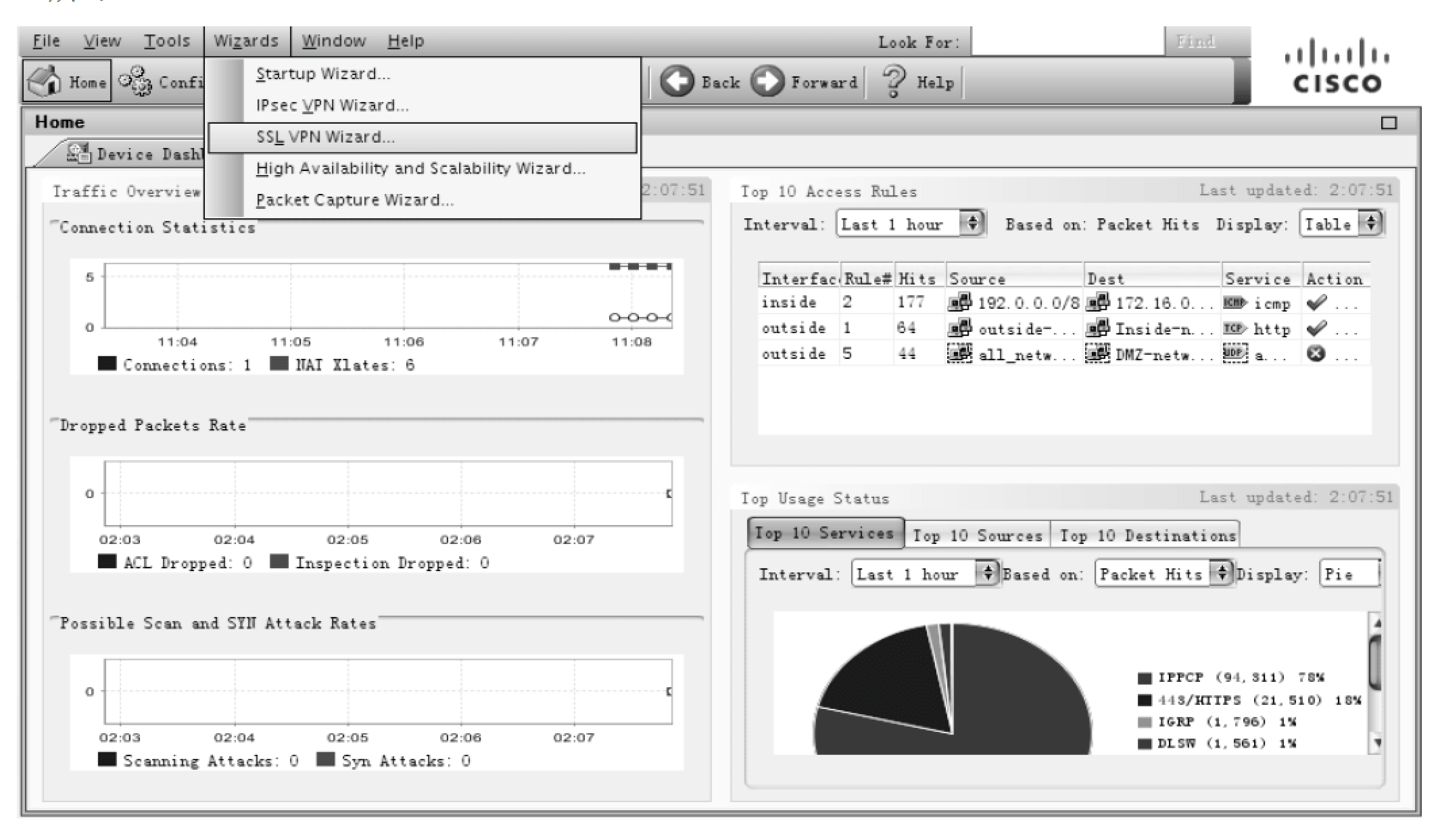


图 10-29　启动 VPN 配置向导

❷ 在 SSL VPN 配置向导的第 1 步，选中 Clientless SSL VPN Access 单选按钮，然后单击 Next 按钮，将弹出 VPN 配置向导第 2 向导页，可以选择 SSL VPN 接口，输入连接名称后，选择接口为外部(Outside)接口。如果需要数字证书，可以在 Certificate 下拉列表框中选择，证书可以在微软 CA 服务器上申请。设置完毕后单击 Next 按钮，如图 10-30 所示。

❸ 在 SSL VPN 配置向导的第 3 步中，选中 VPN 客户端的认证模式，可以选择本地认证，也可以选择使用 RADIUS 服务器进行认证，建议使用 RADIUS 认证方式集中控制用户账号。设置完毕后单击 Next 按钮，如图 10-31 所示。

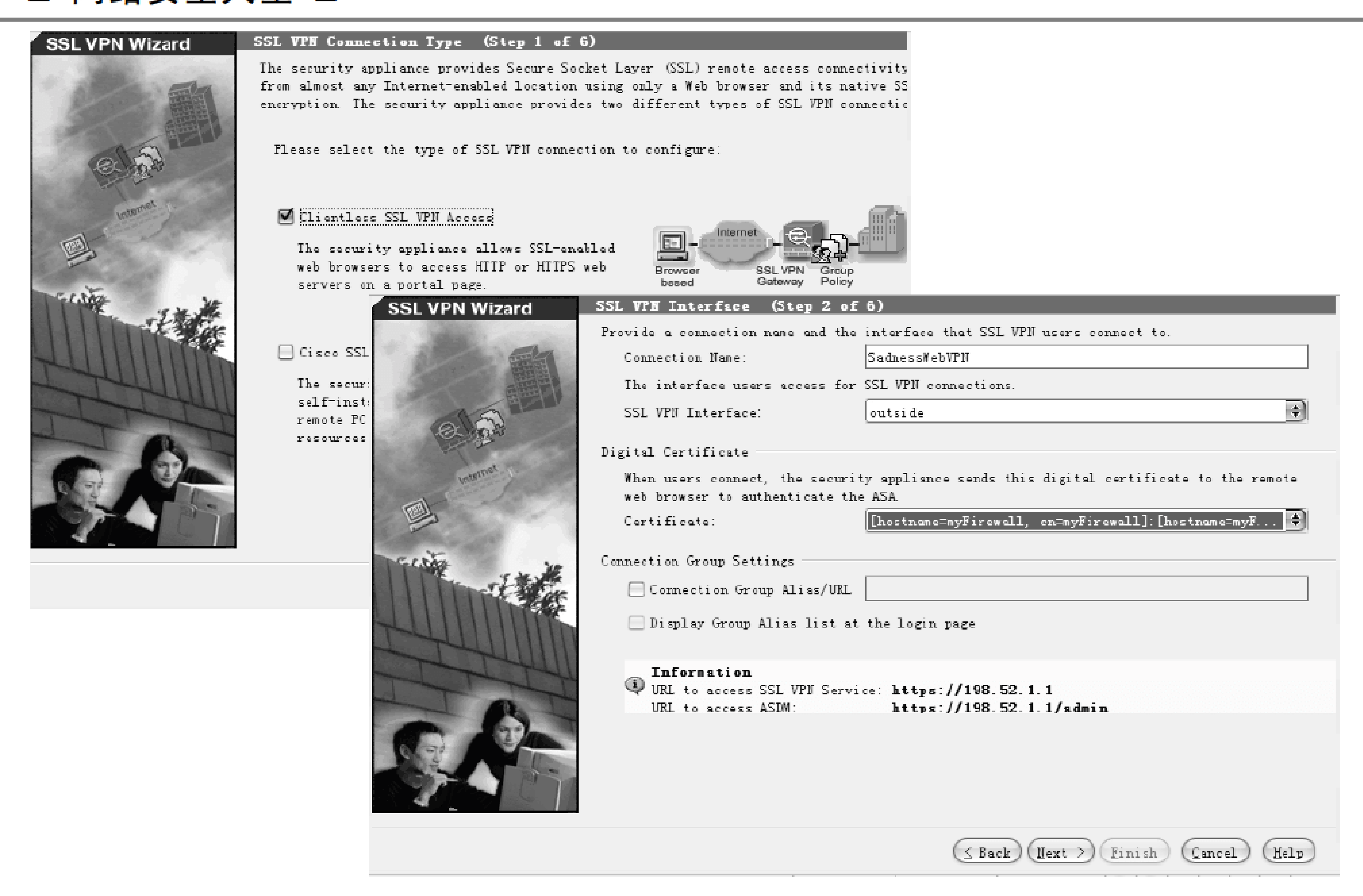


图 10-30　选择 VPN 连接类型模式及 SSL VPN 接口

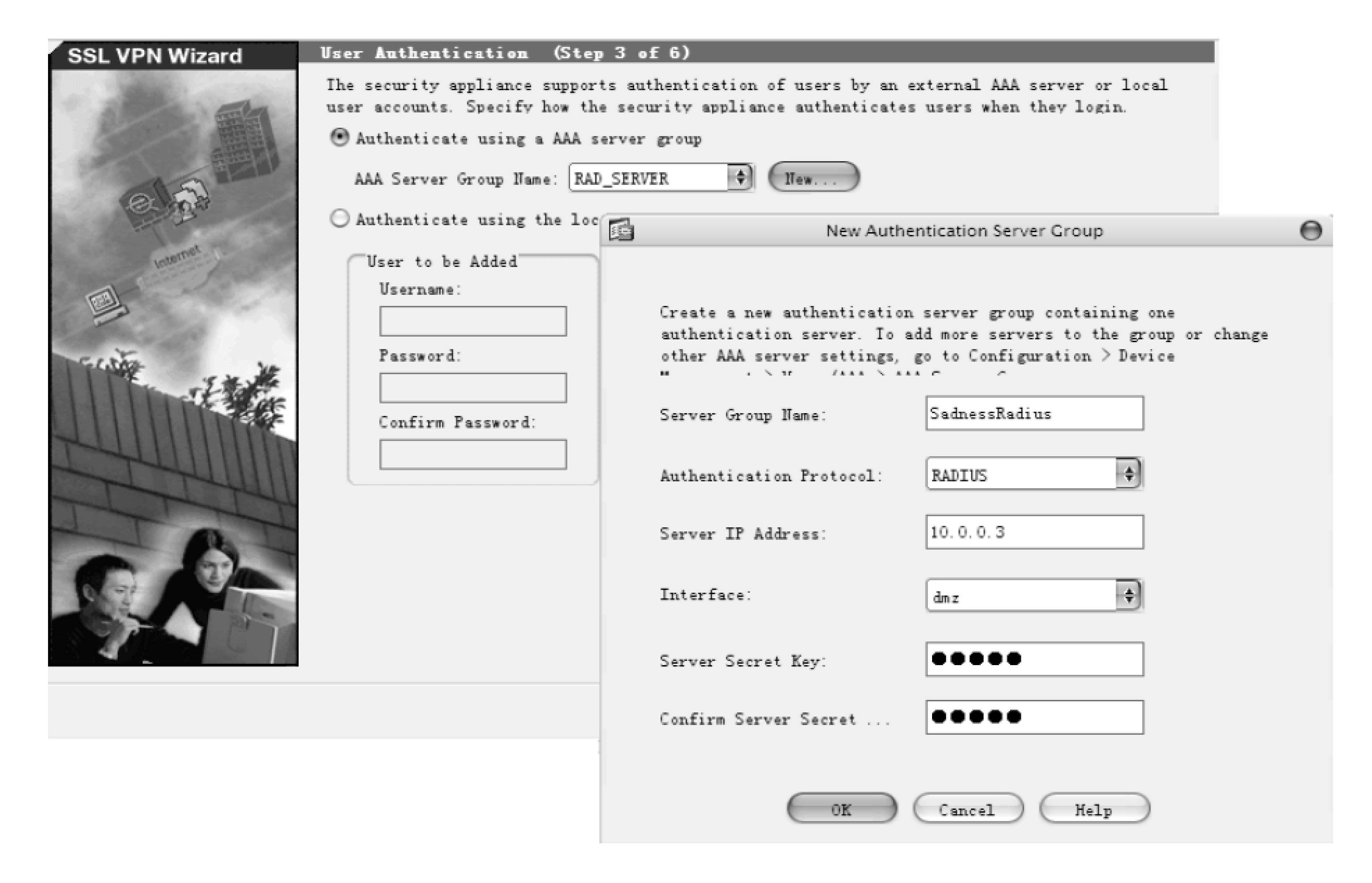


图 10-31　选择 VPN 客户端认证模式

❹ 在 SSL VPN 配置向导的第 4 步中，选中 Create new group policy (创建一个新组策略)单选按钮。设置完毕后单击 Next 按钮，如图 10-32 所示。



图 10-32　选择或创建用户组策略

❺ 在 SSL VPN 配置向导的第 5 步中自定义书签，设置完毕后单击 Next 按钮，如图 10-33 所示。



图 10-33　自定义书签

❻ 在 SSL VPN 配置向导完成后，将显示 Summary 页面，单击 Finished 按钮确认。

2. 配置 RADIUS 服务器

在配置 SSL VPN 时，同样需要配置 RADIUS 服务器以便进行用户认证。下面是配置

Cisco ACS 的过程。

❶ 打开 Cisco ACS 配置页面，单击右侧的 Network Configuration 按钮为 ASA 创建一个 AAA 客户端，如图 10-34 所示。

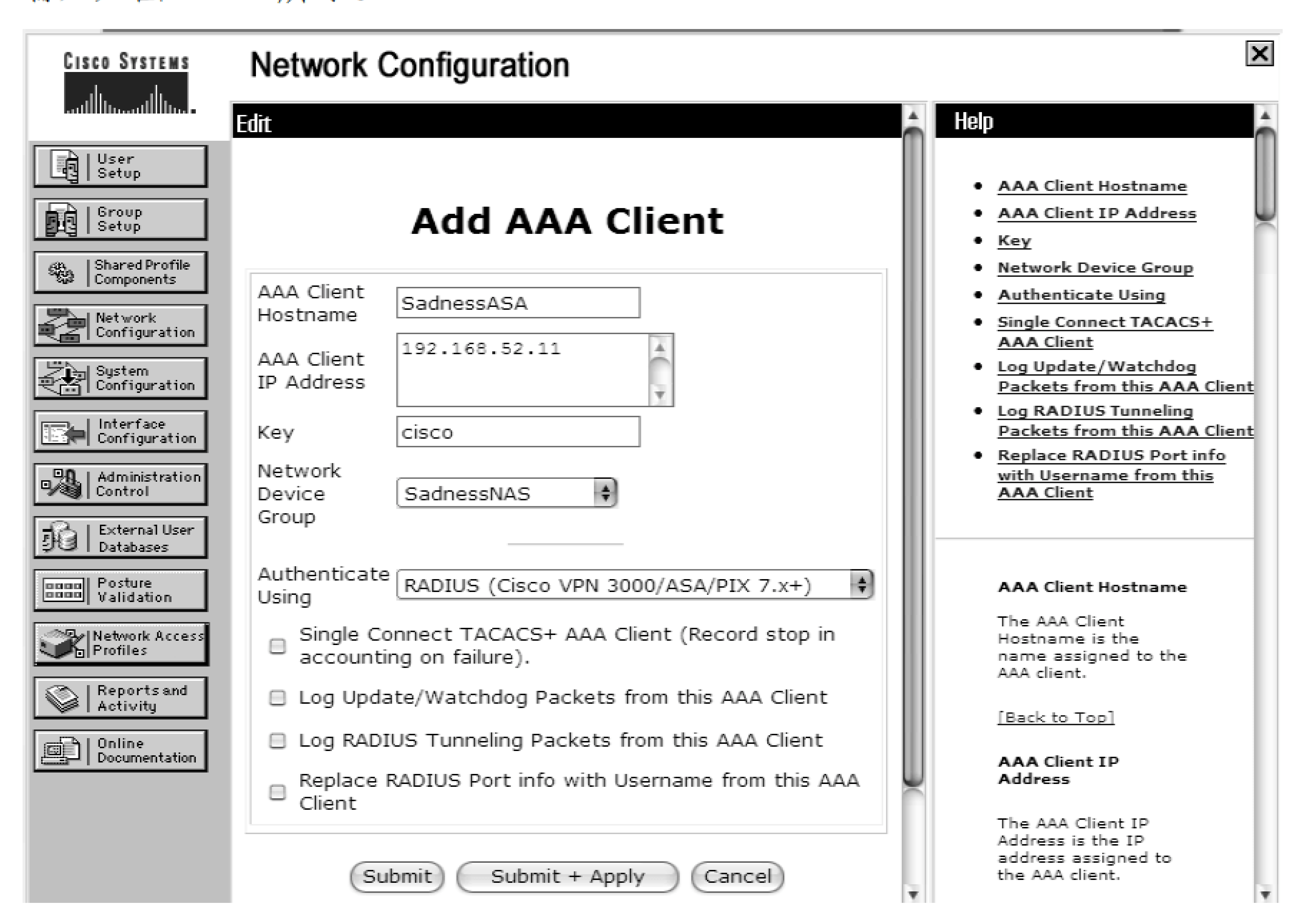


图 10-34 为 ASA 配置 AAA 客户端

❷ 在 Interface Configuration 页面中，设置 RADIUS(Cisco VPN300/ASA/PIX 7.x+)属性，将可能用到的属性选上。例如，[3076\011] Tunneling-Protocols、[3076\071] WebVPN-Url-List、[3076\093] WebVPN-URL-Entry-Enable、[3076\094] WebVPN-File-Access-Enable、[3076\095] WebVPN-File-Server-Entry-Enable、[3076\096] WebVPN-File-Server-Brow sing -Enable，如图 10-35 所示。

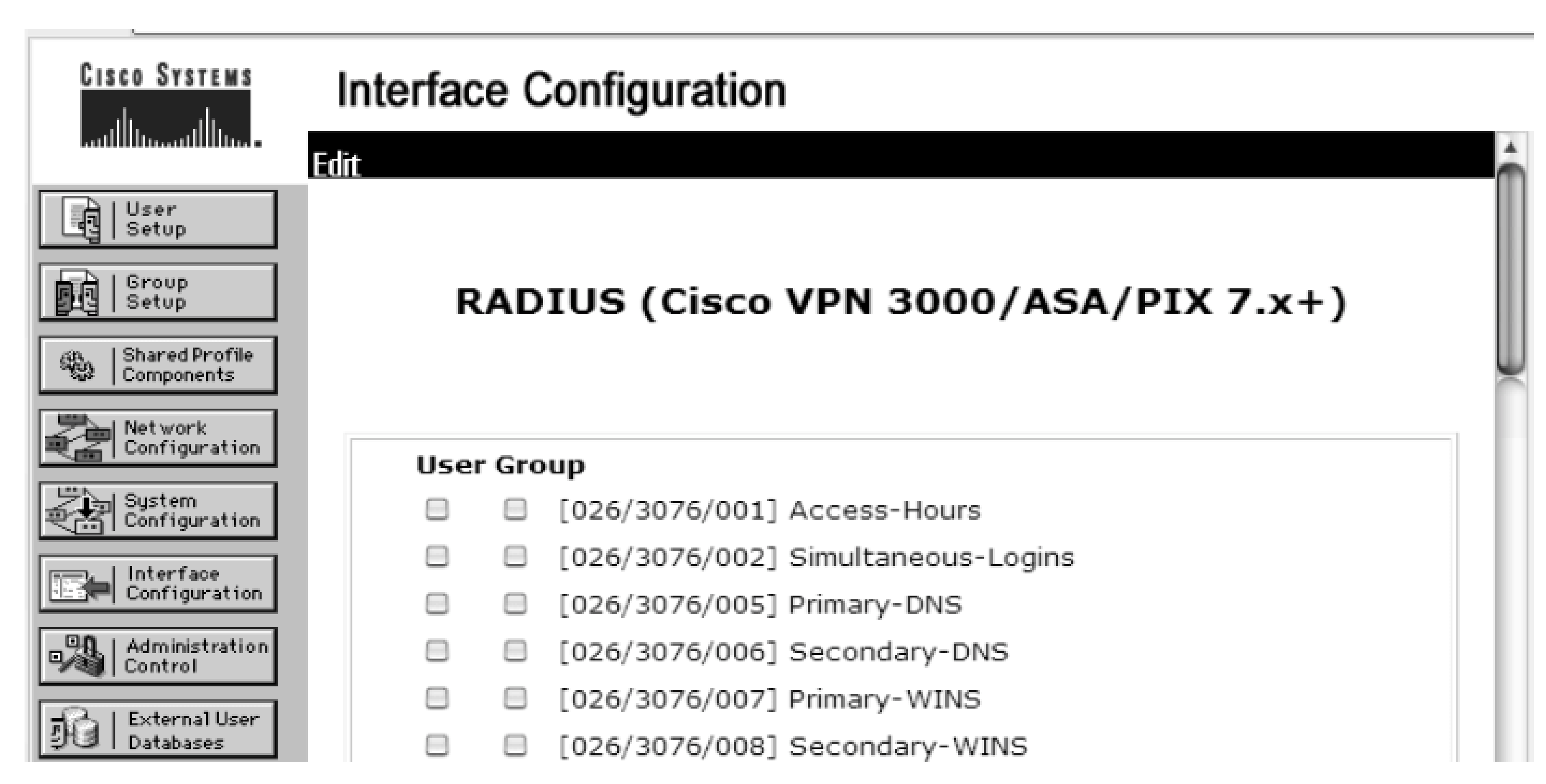


图 10-35 选择 VPN 所用的 RADIUS 属性

❸ 通过浏览器访问 “https://<ASA-IP>”，登录成功后将显示 VPN 工作状态，如图 10-36 所示。

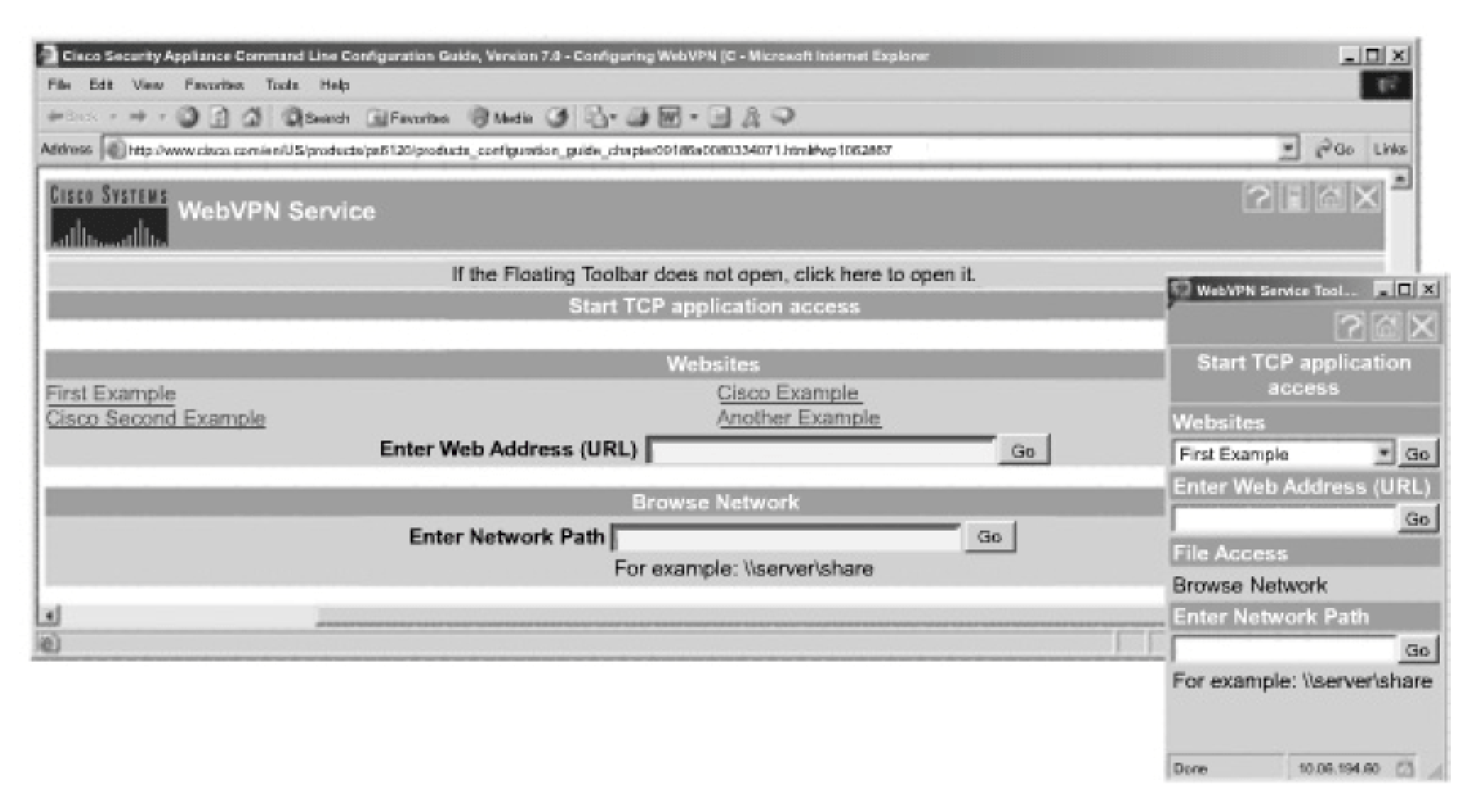


图 10-36　查看 VPN 工作状态

10.5　本 章 小 结

本章讲述了使用 VPN 的一些常用的配置方式，包括站点到站点的 IPSec VPN、员工远程办公所使用的 VPN，以及安全便捷的 SSL VPN。在本章最后还介绍了基于 Linux 的双 ISP 接入 VPN 的配置方式。通过这些配置可以使远程办公室能够安全地连接到公司总部，同时员工也可以方便而安全地连接到公司网络。

第 11 章　统一安全管理

按照前几章所述的方式组建一个安全的园区网络，但是入侵检测系统、防火墙、UTM 等各种安全设备将产生大量的安全日志，并且安全信息系统相对孤立，导致管理员对实时安全信息不了解，无法及时发出预警信息；攻击事件发生后，无法确诊网络故障的原因或感染源/攻击源；网络业务恢复时间长，对某些特定安全事件没有适合的方法，如 DDoS 攻击等。管理员通常使用人工判断，耗费时间和资源，难于作出快速判断和实时响应。因此有必要建设一套自动化的系统来对日志进行统一处理。

通过本章的学习，读者应掌握以下主要内容：

✧　网络监控系统发展历程

✧　统一安全管理的基本概念

✧　CS-MARS 部署及配置方法

✧　事件控制系统的功能

11.1　统一安全管理

应用实例导航：Sadness 公司部署网络流量监控

※场景呈现

某日，Sadness 公司的网络管理员 Jam 对设备流量进行检查，发现流量急剧加大，某些 Live Graph 流量已经出现中断(如图 11-1 所示)，设备被攻击导致死机。Jam 同时发现防火墙、入侵检测系统和 CSA 管理终端发出大量日志，而 Jam 面对海量的日志信息却无从下手。他迫切希望有一种能够统一管理大量日志的设备，并能够帮助管理员作出恰当的处理预案。

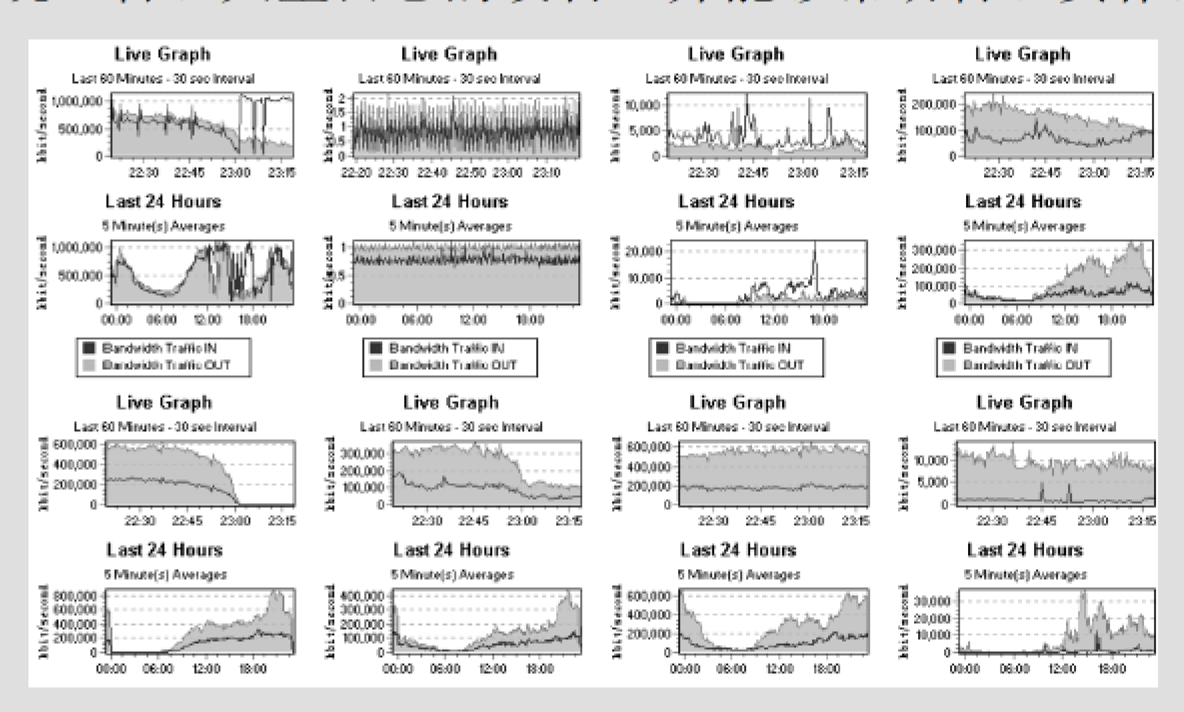


图 11-1　Sadness 网络流量示意图

※技术要领

(1) Syslog/SNMP、NetFlow 和统一安全管理等 3 种网络监控系统的特点；
(2) CS-MARS (Cisco 监控分析响应系统)的部署。

11.1.1 网络监控系统发展历程

1. Syslog/SNMP

最早对于网络设备的监控采用 Syslog 日志的方式，后期使用了基于 SNMP 协议的网络管理系统，在网络管理平台中具有代表性的平台有 SolarWinds、HP Openview、IBM Tivoli 等，这些软件可以接收一些 Syslog 和 SNMP 消息进行处理并绘制图表。例如 MRTG(Multi Router Traffic Grapher)可以通过 SNMP 获得网络设备中的流量信息，并绘制成相应的流量图，如图 11-2 所示。

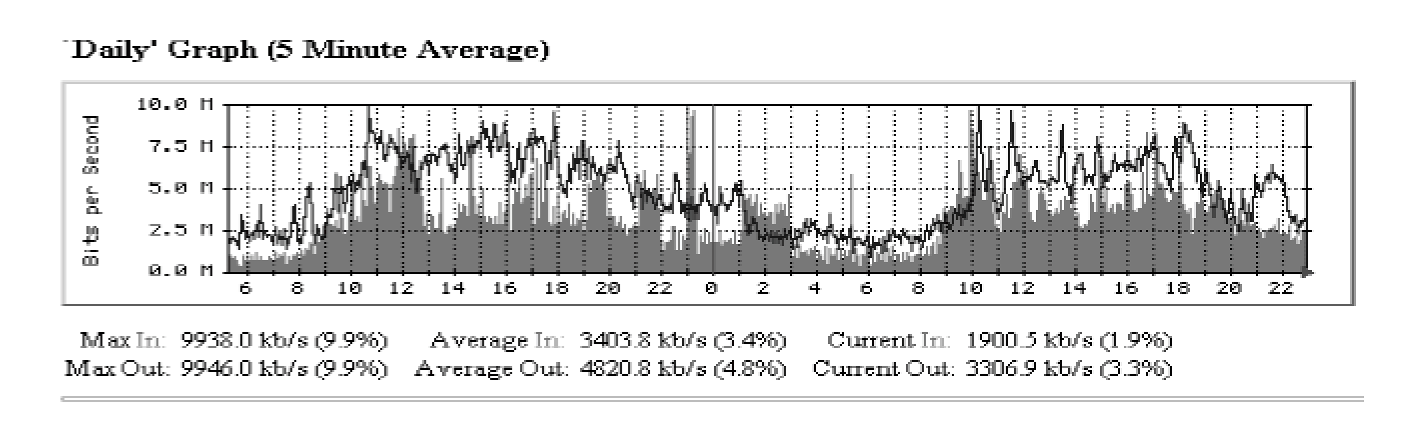


图 11-2 MRTG 流量统计图

国内较多的园区网络都采用基于 MRTG 和 Solarwinds(如图 11-3 所示)等软件的网络管理平台。这类管理平台能实现拓扑展示、关键文件和进程的监控、实时的性能监控、故障报警、故障分析并进行故障定位和处理。但是这类软件仅能在攻击发生后一定时间察觉到流量异常，对于一些小流量的攻击行为根本无法有效地监控。

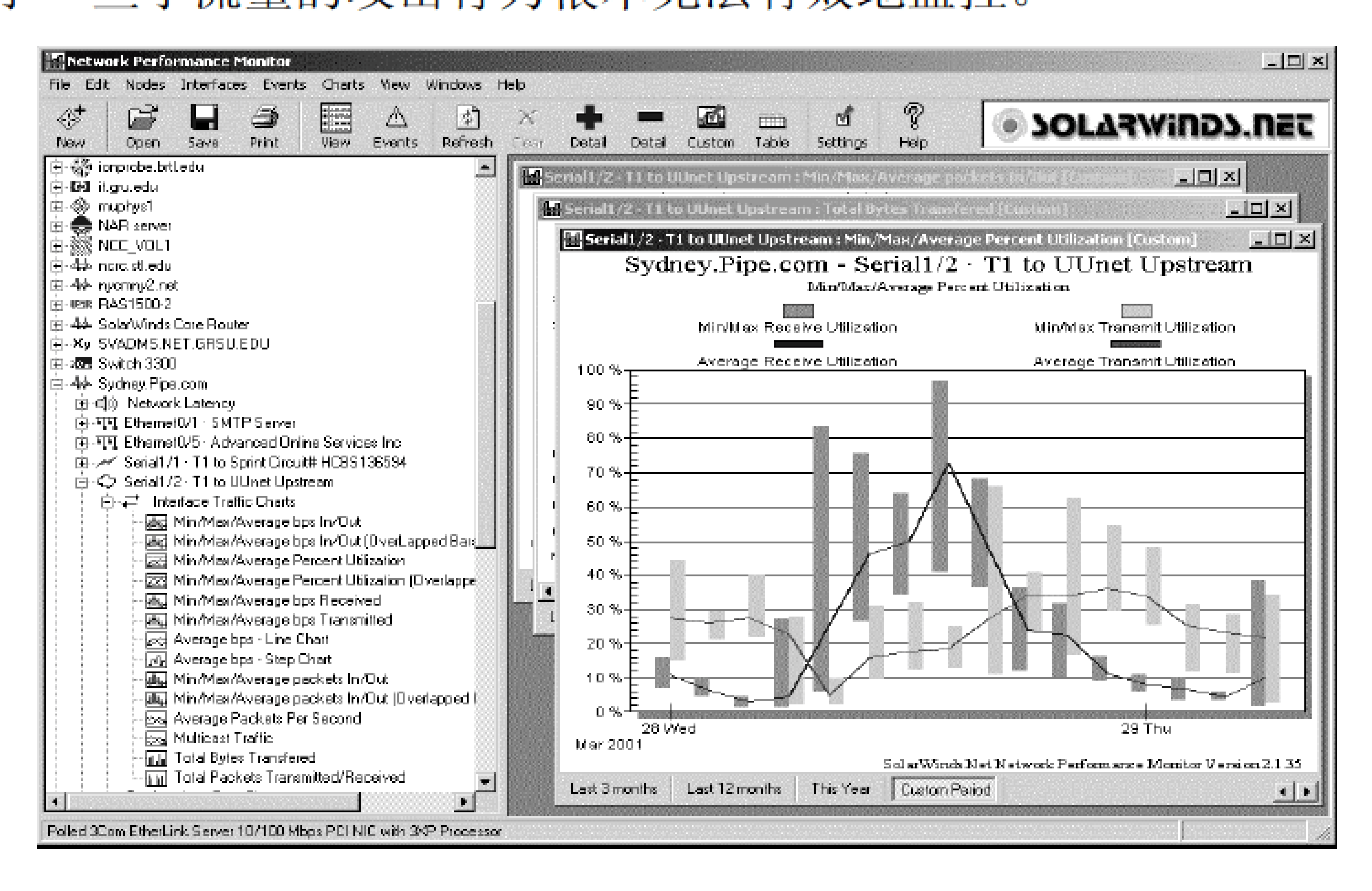


图 11-3 Solarwinds 监控软件

2. NetFlow

NetFlow 是 Cisco 公司提出的网络数据包交换技术，该技术首先被用于网络设备对数据交换进行加速，并可同步实现对高速转发的 IP 数据流(Flow，简称 IP 流)进行测量和统计。经过多年的技术演进，NetFlow 原来用于数据交换加速的功能已经逐步改由网络设备中的专用集成电路(ASIC)芯片实现，而对流经网络设备的 IP 流进行测量和统计的功能却更加成熟，并成为当今互联网领域公认的最主要的 IP 流量分析、统计和计费行业标准。图 11-4 所示的是 NetFlow 操作界面。

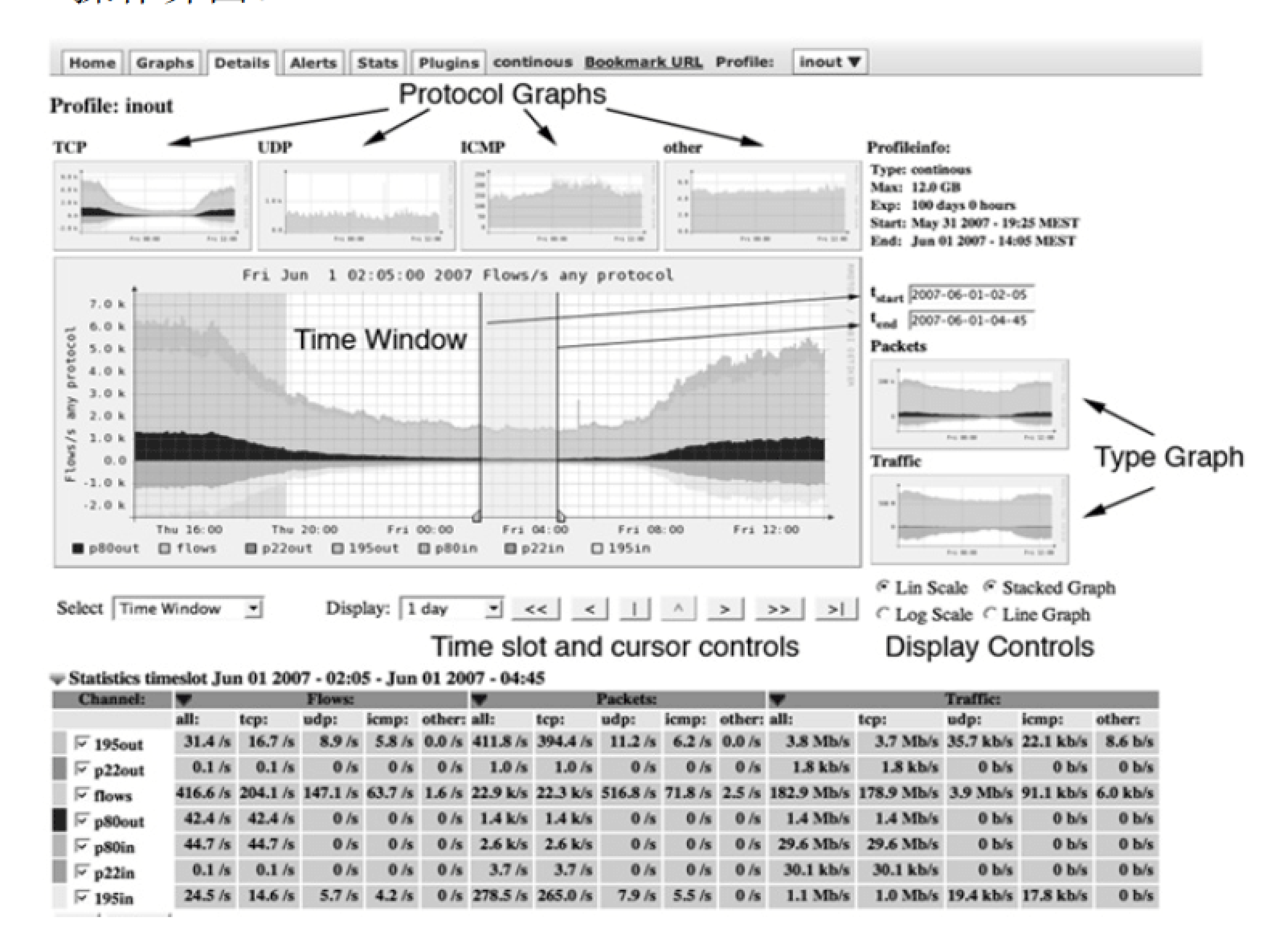


图 11-4　NetFlow 操作界面

为了对运营商网络中不同类型的业务流进行准确地流量和流向分析与计量，首先需要对网络中传输的各种类型数据包进行区分。由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上就构成了运营商网络中某种业务的一个流。如果管理系统能对全网传送的所有 Flow 进行区分，准确记录传送时间、传送方向和流的大小，就可以对运营商全网所有业务的流量和流向进行分析和统计。

通过分析网络中不同流之间的差别，可以发现判断任何两个 IP 数据包是否属于同一个流，实际上可以通过分析 IP 数据包的源 IP 地址、目的 IP 地址、源端口号、目的端口号、第三层协议类型、服务类型(TOS)字节、网络设备输入或输出的逻辑网络端口(ifIndex) 7 个属性来实现。

Cisco 公司的 NetFlow 技术就是利用分析 IP 数据包的上述 7 个属性，快速区分网络中传送的各种不同类型业务的流。对区分出的每个流，NetFlow 技术可以进行单独跟踪和准确计量，记录其传送方向和目的地等流向特性，统计其起始和结束时间、服务类型、包含的数据包数量和字节数量等流量信息。

NetFlow 具有强大的统计功能，因此对于一些异常事件可以较为容易地反映出攻击流量所使用的协议和端口，方便用户进行快速响应。同时借助 NetFlow 的信息，可以有效地构建 DDoS 清洗中心(例如第 9 章中介绍的 DDoS 防御系统)等。

3. 统一安全管理

随着企业业务逐渐转移到互联网上，企业对于这些业务的保障需求也日益提高，因此一系列安全改造项目获得执行，同时大量的网络安全设备加入到企业网络中。但是，网络管理员将面临众多设备的日志却无法进行处理，当攻击发生后，可能 IPS/IDS 会主动进行报警，而管理员由于一些低端 IPS/IDS 误报率较高，而无法完全信任这些日志。同时伴随着 NetFlow 等监控软件报告流量异常，网络管理员也有可能认为这是公司的正常业务流量而忽视攻击行为，即便是防火墙的报警，网络管理员也因为某些防火墙经常报告攻击事件而忽视真正的攻击发生。

网络管理员在大量网络设备发出的相对孤立的日志中查找出攻击行为相当困难。同时这也使得管理员缺乏整个网络的意识，仅局限于某个孤立设备上，无法有效而快速地处理攻击事件。IT 管理者们更希望在问题发生的时候，得到一个综合全面的安全报告，以了解企业网络到底处于什么样的状态，遭受过什么样的攻击，正面临着什么样的危险？而不是每一个产品信息的简单罗列，企业需要一个能集中管理所有产品信息、智能化的安全管理中心。

单纯从技术的角度而言，目前业界比较认可的安全网络的主要环节包括入侵防护、入侵检测、事件响应和系统灾难恢复。入侵防护主要是在安全风险评估和对安全威胁充分了解的基础上，根据对安全的期望值和目标制定相应的解决方案。入侵检测主要是通过对网络和主机中各种有关安全信息的采集和及时分析，发现网络中的入侵行为或异常行为，及时提醒管理员采取响应动作以阻止入侵行为的继续。事件响应是当发生安全事件的时候所采取的处理手段，与入侵防护和入侵检测不同，事件响应主要体现为专业人员的服务和安全管理。系统灾难恢复是指如何在数据、系统或者网络由于各种原因受到损害后，尽快恢复损失前的状态。除此之外，风险评估、安全策略和管理规定等，经常也被作为安全保障的重要部分。

但是不论有多少环节，要想实现安全的网络，风险评估、策略制定、入侵防护和入侵检测等都是应急响应的准备工作，有了这些准备工作，事件响应才可以及时得到各种必要的审计数据，进行准确的分析，采取措施降低损失或者追踪入侵者的来源等。因此，事件响应实际上将各个环节贯穿起来，使得不同的环节互相配合，共同实现安全网络的最终目标。而事件响应能否在攻击者成功达到目标之前有效地阻止攻击和快速响应，不但取决于安全产品本身采取的技术，更取决于使用和管理产品的人员以及网络安全信息管理平台。优秀的信息管理分析工具，可以让安全管理人员对网络的安全状态了如指掌，快速行动，真正实现安全网络。

CS-MARS 是一个较为成熟的安全管理平台，它可以作为多种网络平台。

- ✧ 交换机路由器平台：Cisco IOS 11.x 或 12.x、Catalyst OS 6.x、NetFlow v5/v7、NAC ACS 3.x、Extreme Extremeware 6.x 等。
- ✧ 防火墙/VPN 平台：Cisco PIX 7.x、IOS Firewall、FWSM 1.x/2.2、VPN Concentrator

4.x、Cisco ASA、CheckPoint Firewall-1 NG FPx、 VPN-1、NetScreen Firewall 4.x/5.x、Nokia Firewall 等。

- ✧ IPS/IDS 平台：Cisco NIDS 3.x/4.x/5.x、IDSM 3.x& 4.x/5.x、Enterasys Dragon NIDS 6.x、ISS RealSecure Network Sensor 6.5/7.0、Snort NIDS 2.x、McAfee Intrushield NIDS 1.x、NetScreen IDP 2.x、Symantec ManHunt 3.x 等。
- ✧ 漏洞评估软件：eEye REM 1.x、Foundstone FoundScan 3.x 等。
- ✧ 主机安全软件：Cisco Security Agent (CSA) 4.x、McAfee Entercept 2.5/4.x、ISS RealSecure Host Sensor 6.5/7.0、Symantec AnitVirus 9.x 等。
- ✧ 操作系统的系统记录：Windows NT、2000、2003(有代理和无代理)、Solaris、Linux。
- ✧ 应用服务器平台：Web 服务器 (IIS， iPlanet， Apache)、Oracle 9i&10i 数据库审查记录、Network Appliance NetCache 等。

图 11-5 所示的是 CS-MARS 的外观。



图 11-5　CS-MARS 的外观

通过对大量系统的支持，CS-MARS 可以将成千上万的日志信息进行标准化处理，并汇报成一系列攻击报告。同时，对于每个可能的攻击进行自动地脆弱性扫描，检查攻击是否成功到达目标，目标是否的确可能遭受攻击。自动脆弱性扫描会使用关于终端系统的信息发现误报，制定规则以减少将来对可能攻击的分析和处理。

CS-MARS 可以利用网络拓扑发现同一个进程的不同事件和流程。这些事件可能由跨越 NAT 边界的网络设备生成，因而可能拥有不同的源及(或)目的地地址和端口。CS-MARS 所采用的、已经申报专利的算法可以利用拓扑知识和设备配置信息，将这些设备事件关联到同一个进程。这可以减少事件数据，创造出整个攻击环境。

同时它可以利用网络拓扑减少误报。通过识别同一个进程的事件并分析某个攻击从源到目的地的拓扑路径，CS-MARS 可以发现某个攻击是否的确到达了预定的目的地，或者被某个中间设备(例如防火墙或者入侵防范设备)所丢弃。

由于 CS-MARS 的部署方式，使得它可以利用网络拓扑发现最理想的防御点。通过分析从攻击者到预定目的地的路径，CS-MARS 可以将距离攻击者最近的设备定为最理想的防御点。设备配置信息还让 CS-MARS 可以生成准确的、针对设备的防御命令。

CS-MARS 还可以利用网络拓扑发现攻击路径和网络热点。CS-MARS 能够用网络拓扑知识找出攻击的拓扑路径，发现攻击者和攻击主机所在的网络区域,并且利用网络拓扑提高证据分析能力，如图 11-6 所示。因为 CS-MARS 可以从网络配置了解 NAT，所以它可以通过识别 NAT 地址解析和攻击者 MAC 地址大大增强证据分析能力。

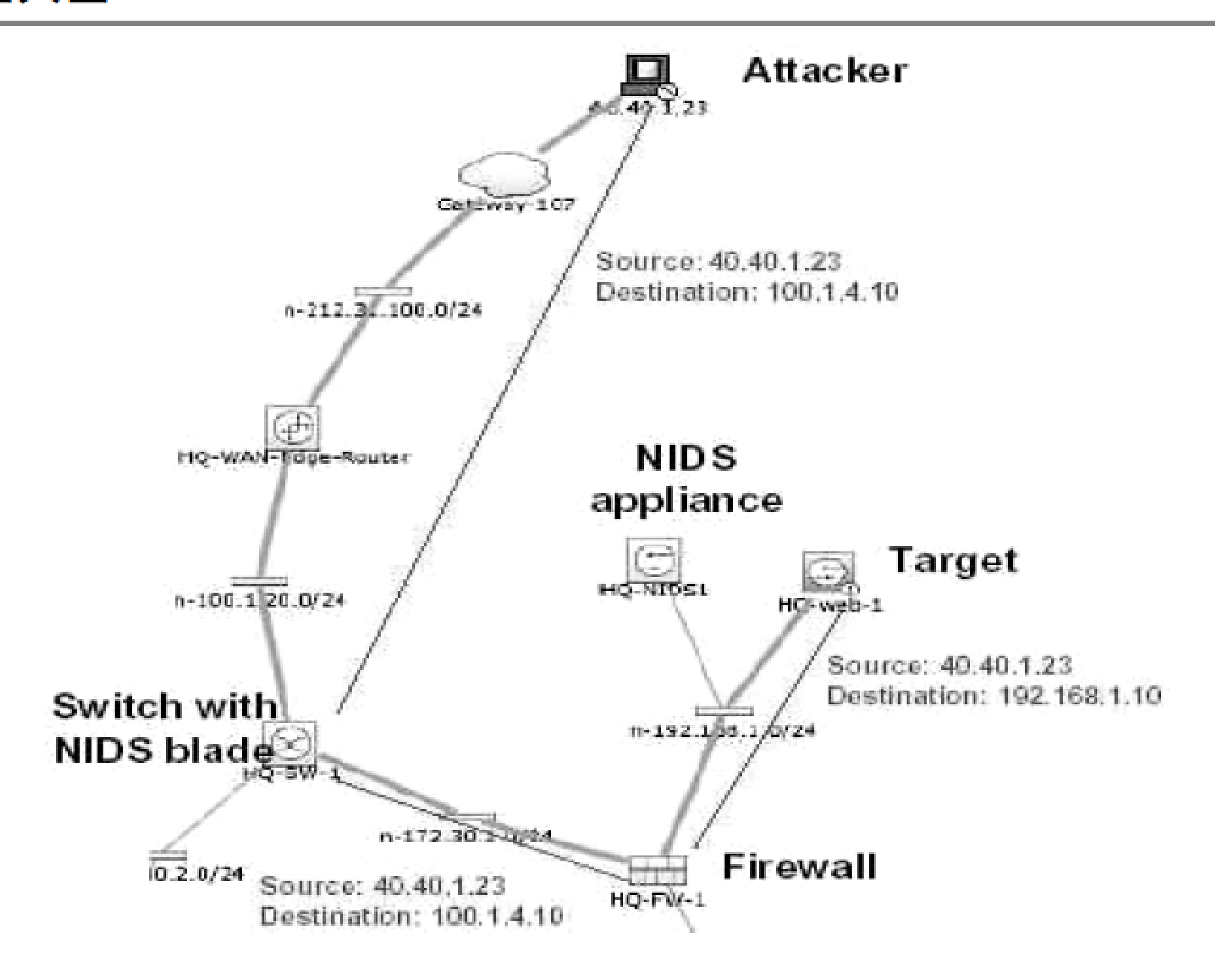


图 11-6　攻击路径

11.1.2　配置 CS-MARS

下面以 CS-MARS 为例，简要介绍一下统一安全管理的实施过程。

❶ 对于一台新的 CS-MARS，由于没有配置 IP 地址等参数，只能使用 Console 端口进行配置。利用 Console 端口配置 CS-MARS 时，超级终端的参数设置如图 11-7 所示。



图 11-7　配置超级终端

❷ 启动 CS-MARS 后，输入正确的用户名和密码，便可登录到 CS-MARS。在默认情况下，登录 CS-MARS 的用户名和密码都是“pnadmin”。

```
+-----------------------------------------------------------------------+
+                                        +
+   Protego MARS - Mitigation and Response System   +
+           version : 4 . 2 . 1 (2250)          +
+------------------------------------------------------------------------+
CS-MARS  login:  pnadmin
```

```
Password:
Last login: Wed Mar 26 16:36:20 2007
  CS MARS - Mitigation and Response System
    ? for list of commands
[pnadmin]$
```

❸ 根据 CS-MARS 的部署位置，配置合适的 IP 地址、默认网关和系统时间。需要注意，CS-MARS 的时间一定要与系统其他设备一致。

```
[pnadmin]$ ifconfig eth0 192.168.0.100 255.255.255.0
[pnadmin]$ ifconfig eth1 192.168.1.100 255.255.255.0
[pnadmin]$ gateway 192.168.1.254
[pnadmin]$ date 09/11/07
[pnadmin]$ time 11:32:33
```

❹ 使用 ifconfig 命令验证上述配置。此后，对 CS-MARS 便可以使用 SSH 实施远程管理。

```
[pnadmin]$ ifconfig
eth0 Link encap:Ethernet  HWaddr 00:05:50:9C:74:45
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5969 (5.8 Kb)  TX bytes:4410 (4.3 Kb)
          Interrupt:10 Base address:0x1080
eth1 Link encap:Ethernet  HWaddr 00:0C:29:68:48:83
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:343 errors:0 dropped:0 overruns:0 frame:0
          TX packets:153 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27013 (26.3 Kb)  TX bytes:16514 (16.1 Kb)
          Interrupt:9 Base address:0x1400
```

❺ 开启网络中的交换机和路由器的 Syslog 和 SNMP 服务，以便于 CS-MARS 获取系统日志。

```
Router(config)# logging on
Router(config)# logging trap debugging
Router(config)# logging 191.168.1.100
Router(config)# snmp-server community cisco RO
Router(config)# snmp-server host 191.168.1.100 cisco syslog
```

❻ 开启网络中的交换机和路由器的 NetFlow 功能。

```
Router(config)#ip flow-export source FastEthernet 0/0
Router(config)#ip flow-export destination 192.168.1.100 9999
Router(config)#ip flow-export version 5
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
```

❼ 如果网络中还 ASA 调协，也需要开启 Syslog 和 SNMP 服务。

```
logging enable
logging timestamp
logging emblem
logging monitor debugging
logging buffered notifications
logging trap warnings
```

```
logging history warnings
logging host inside 192.168.1.100 format embleminterface gigabitEthernet 0/0
snmp-server host inside 192.168.1.100 poll community cisco
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown coldstart
snmp-server enable traps syslog
snmp-server enable traps ipsec start stop
snmp-server enable traps remote-access session-threshold-exceeded
```

8 打开 IE 浏览器，在地址栏中输入“https://<cs-mars-ip-address>”登录到 CS-MARS，如图 11-8 所示。

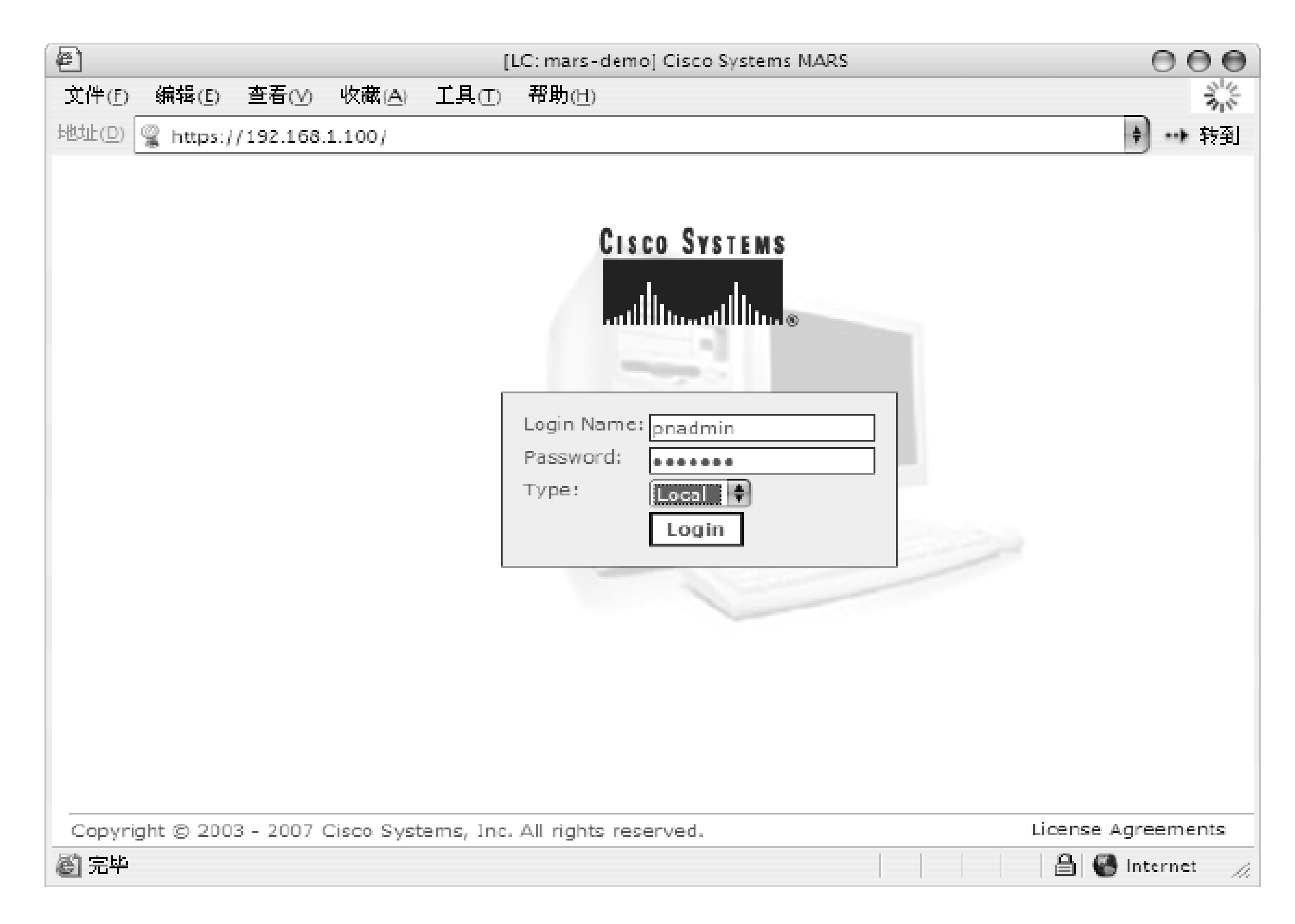


图 11-8 登录 CS-MARS

9 登录成功后，选择 ADMIN 页面，单击 Security and Monitor Devices 链接，将网络中所有 CS-MARS 支持的网络设备添加进去，如图 11-9 所示。

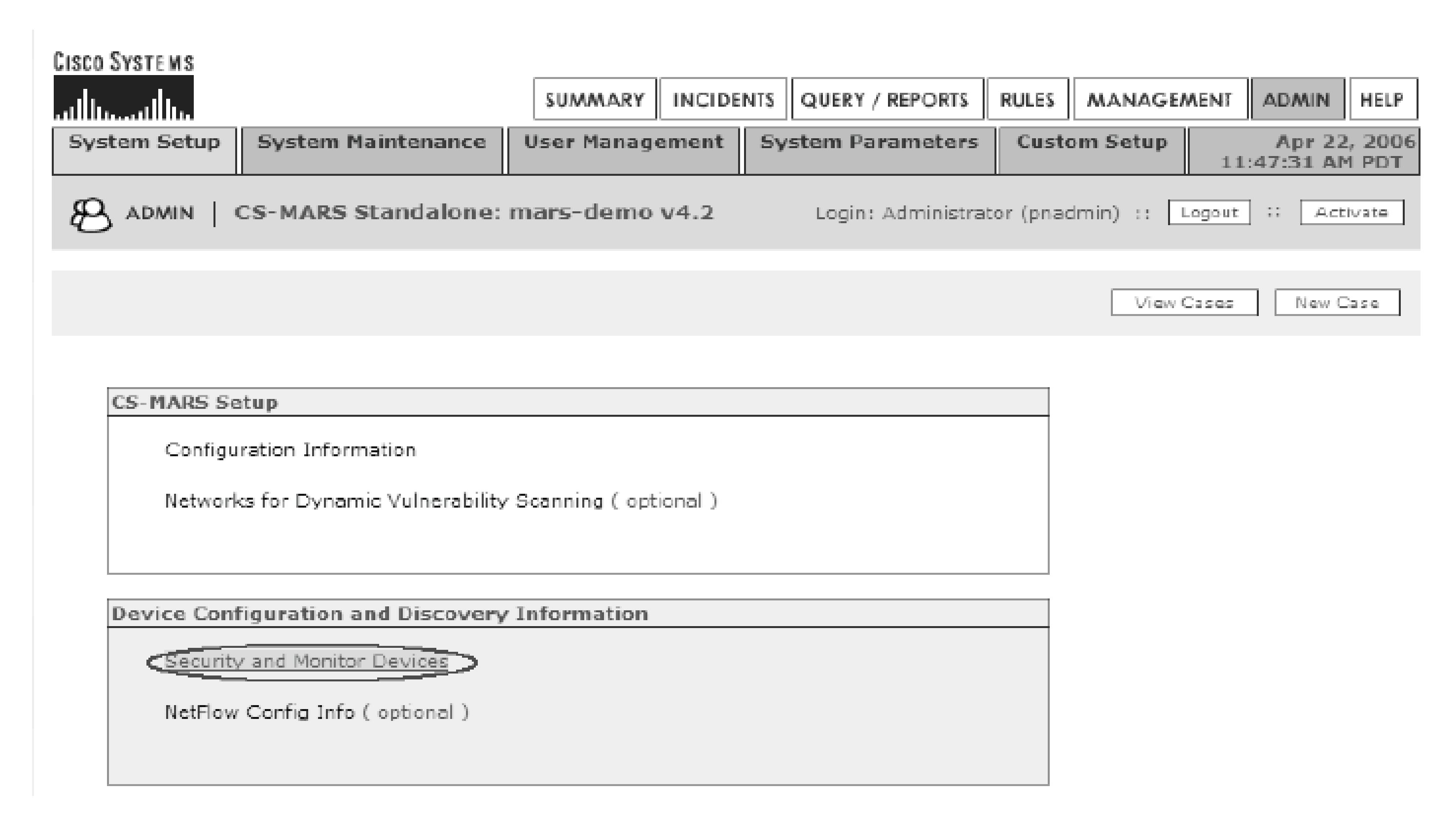


图 11-9 添加设备

10 单击 Add 按钮，在下拉列表框中选择设备类型，并配置相应的 SNMP 参数，单击 Next 按钮，如图 11-10 所示。

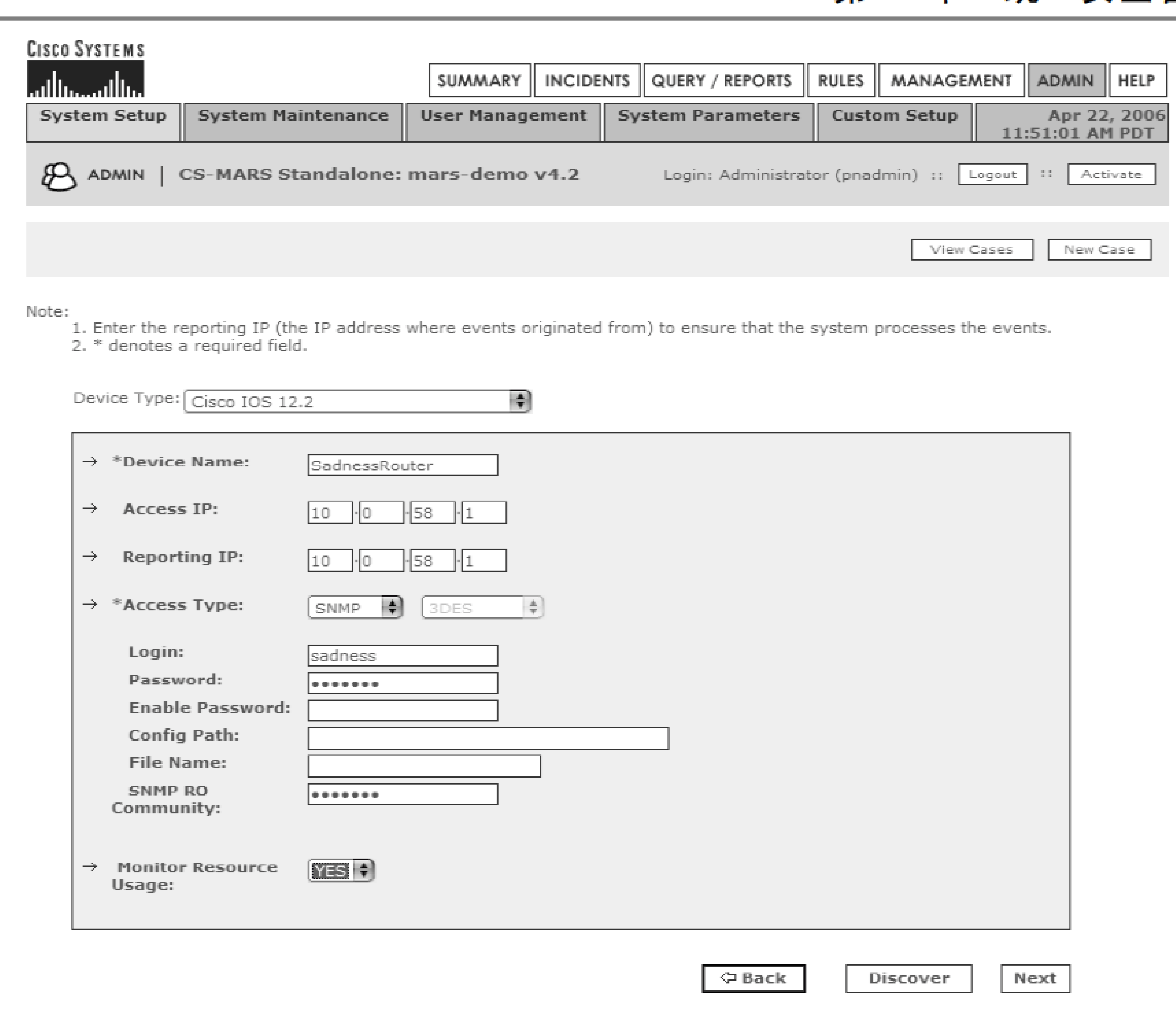


图 11-10　添加设备

⓫ 如果配置了 IOS 集成的 IPS，则需要单击 Add IPS 按钮， 如图 11-11 所示。

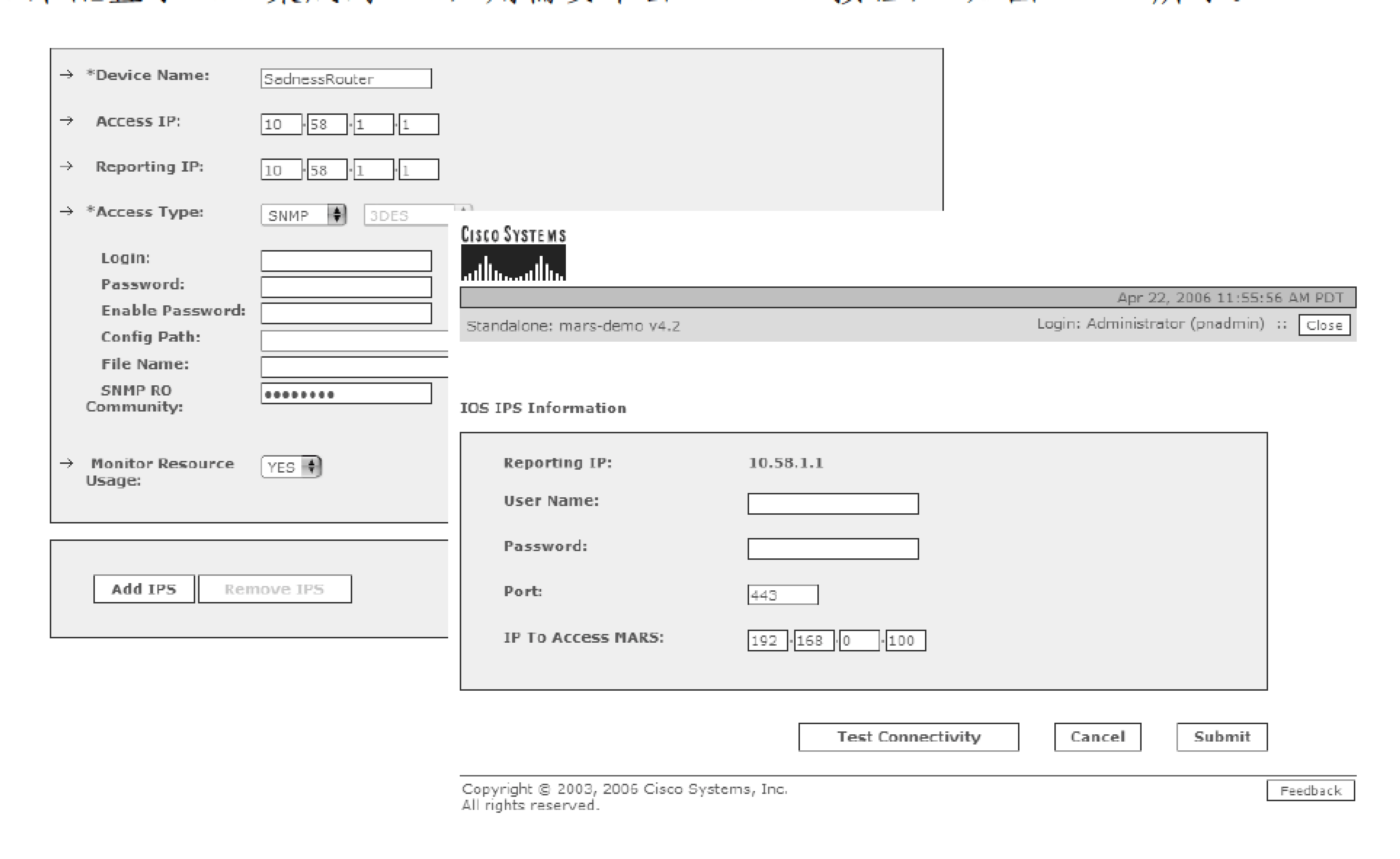


图 11-11　添加 IPS

⓬ 所有网络设备添加完成后，就可以看到设备列表，如图 11-12 所示。

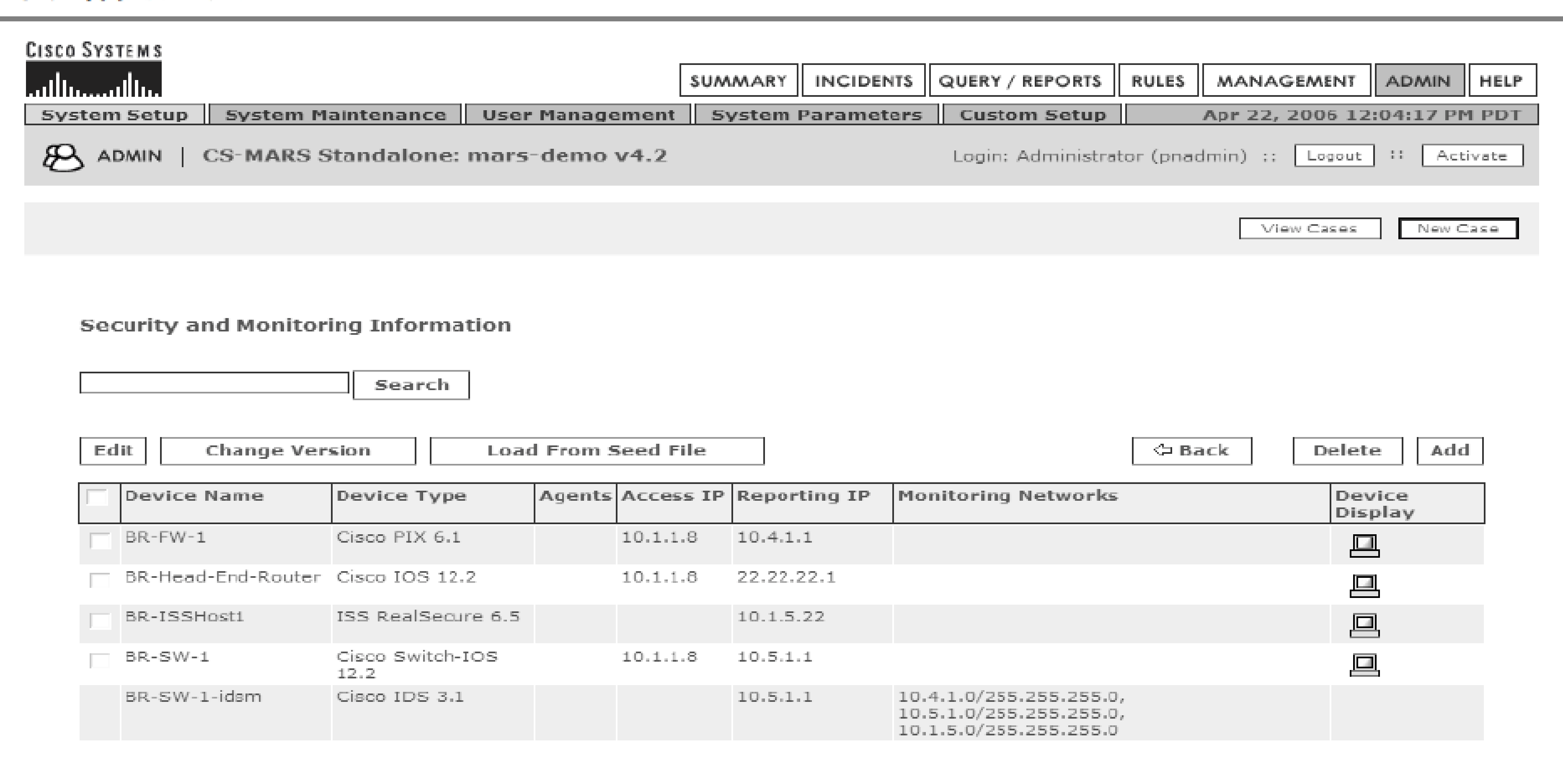


图 11-12　查看设备列表

❸ 添加完成后，依次单击 Admin →Topology/Monitored Device Update Scheduler 链接，升级网络拓扑，如图 11-13 所示。

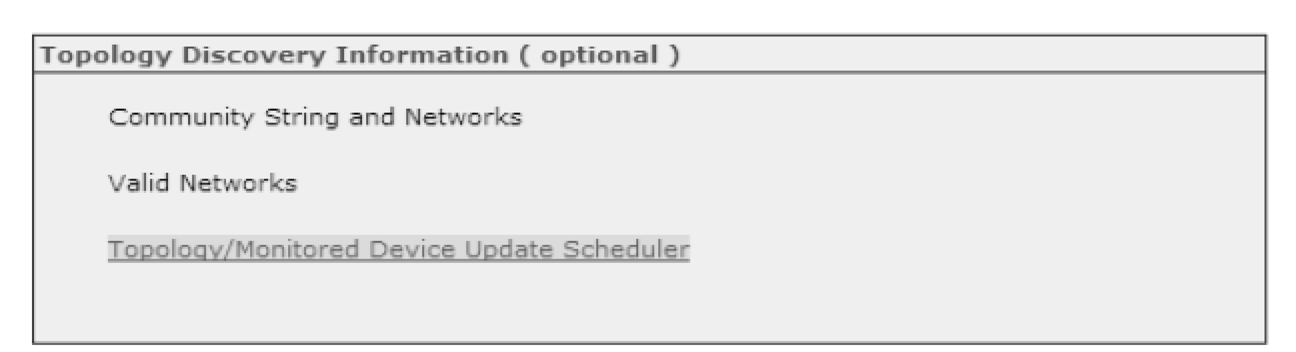


图 11-13　升级拓扑

❹ 网络拓扑升级完成后，可以单击 Summary 链接查看网络拓扑，如图 11-14 所示。

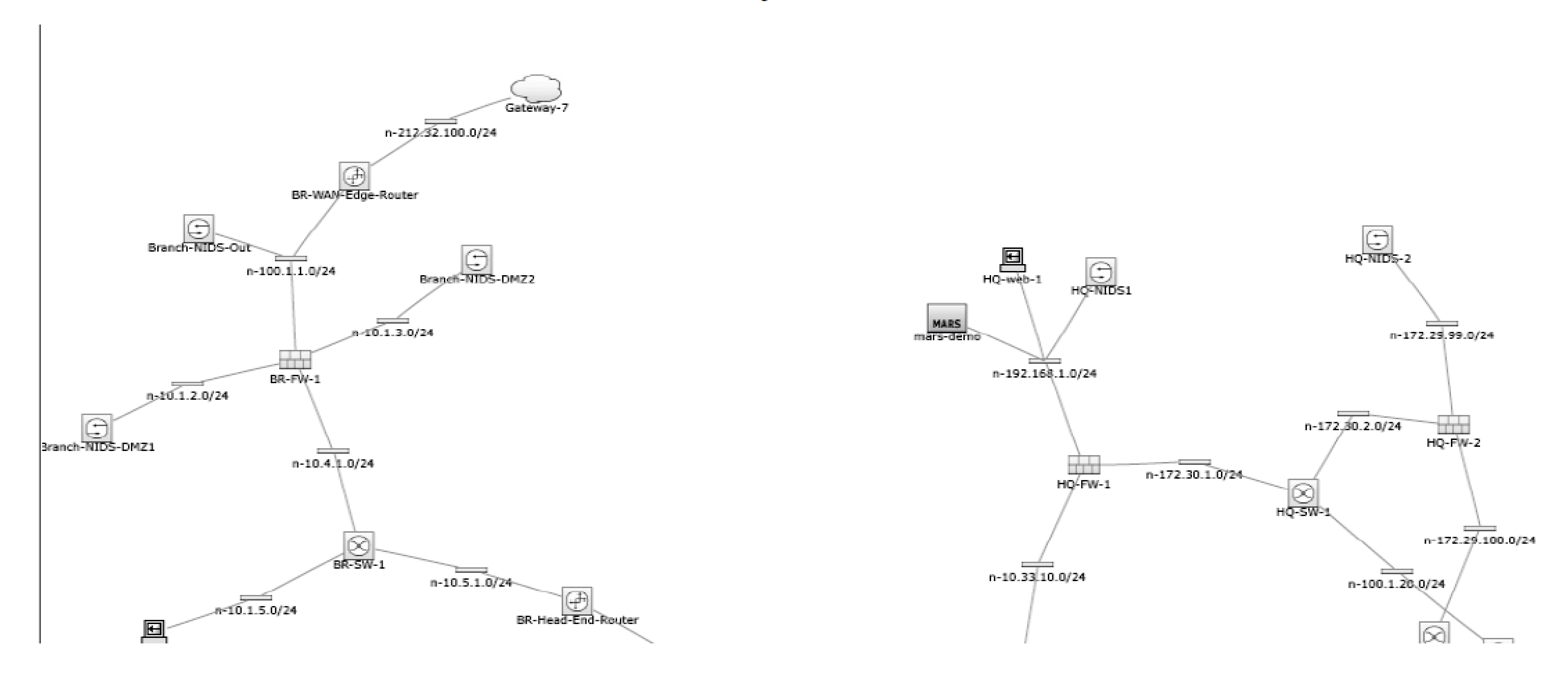


图 11-14　查看网络拓扑

❺ 当网络被攻击时，就可以看到详细的攻击信息，如图 11-15 所示。

❻ 在图 11-15 中单击 My Reports 按钮，可以看到最近攻击事件列表，如图 11-16 所示。

❼ 单击其中一个事件，可以显示出详细的信息，如图 11-17 所示。

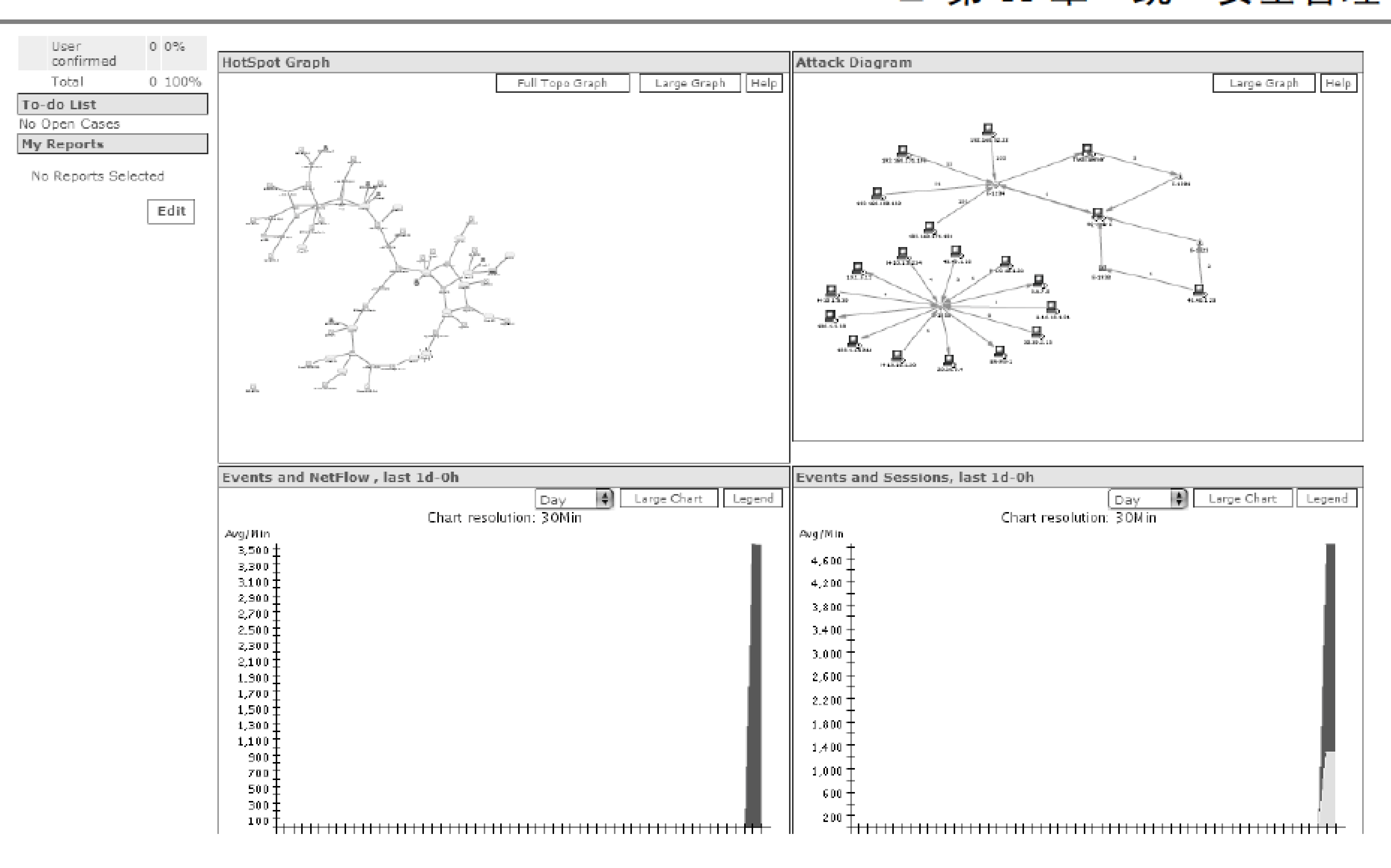
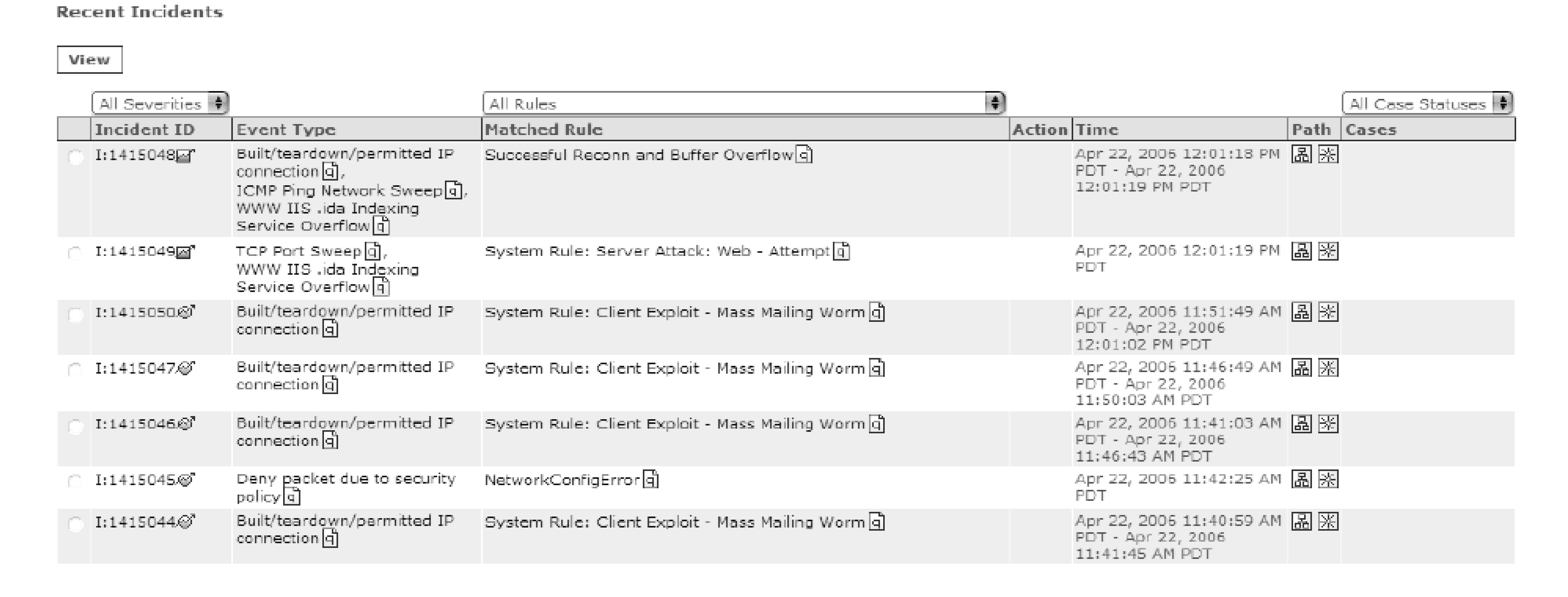


图11-15　攻击拓扑



Recent Incidents

View

All Severities | All Rules | All Case Statuses

	Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
	I:1415048	Built/teardown/permitted IP connection, ICMP Ping Network Sweep, WWW IIS .ida Indexing Service Overflow	Successful Reconn and Buffer Overflow		Apr 22, 2006 12:01:18 PM PDT - Apr 22, 2006 12:01:19 PM PDT		
	I:1415049	TCP Port Sweep, WWW IIS .ida Indexing Service Overflow	System Rule: Server Attack: Web - Attempt		Apr 22, 2006 12:01:19 PM PDT		
	I:1415050	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 22, 2006 11:51:49 AM PDT - Apr 22, 2006 12:01:02 PM PDT		
	I:1415047	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 22, 2006 11:46:49 AM PDT - Apr 22, 2006 11:50:03 AM PDT		
	I:1415046	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 22, 2006 11:41:03 AM PDT - Apr 22, 2006 11:46:43 AM PDT		
	I:1415045	Deny packet due to security policy	NetworkConfigError		Apr 22, 2006 11:42:25 AM PDT		
	I:1415044	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 22, 2006 11:40:59 AM PDT - Apr 22, 2006 11:41:45 AM PDT		

图 11-16　查看最近攻击事件

Rule Name: **Successful Reconn and Buffer Overflow**　　**Status:** Active
Action: None　　**Time Range:** 0h:05m
Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	None	ANY	ANY	1		OR
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/Stealth	ANY	None	ANY	ANY	1		FOLLOWED-BY
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/Login, Penetrate/BufferOverflow/Web	ANY	None	ANY	ANY	1		FOLLOWED-BY
4		$TARGET01	ANY	ANY	Info/AllSession	ANY	None	ANY	ANY	1		

Incident ID: 1415048　　Expand All　Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		ICMP Ping Network Sweep	40.40.1.23	0	192.168.1.10	0	ICMP	Total: 2				
1	S:1390802, *I:1415048*	ICMP Ping Network Sweep	40.40.1.23	0	192.168.1.10	0	ICMP	Apr 22, 2006 12:01:18 PM PDT	HQ-SW-1-idsm			False Positi
1	S:1390803, *I:1415048*	ICMP Ping Network Sweep	40.40.1.23	0	192.168.1.10	0	ICMP	Apr 22, 2006 12:01:19 PM PDT	HQ-NIDS1			False Positi

图11-17　攻击事件

⑱ 单击红色按钮，可以显示出攻击路径，如图 11-18 所示。

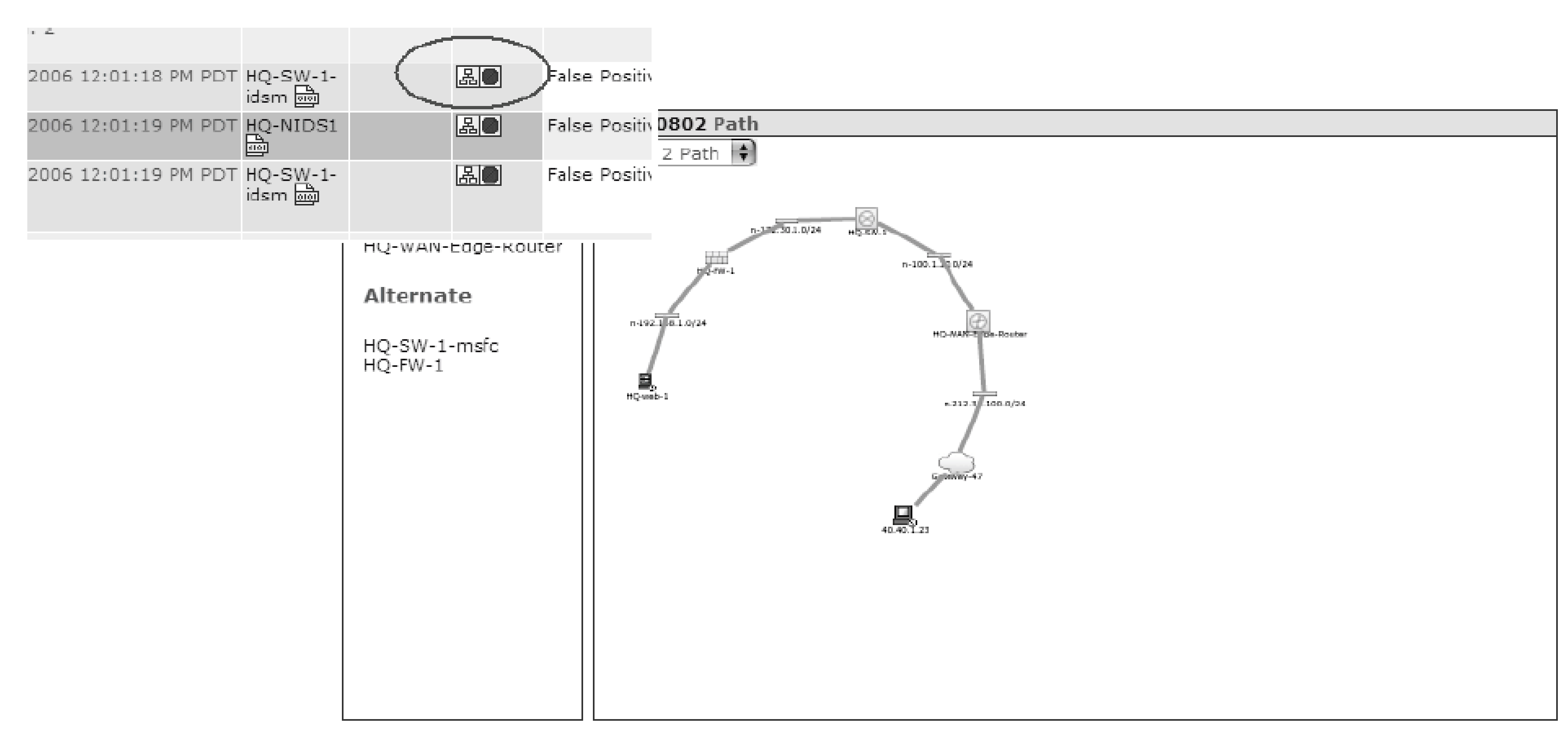


图 11-18　攻击路径

⑲ 同时，在窗口的下方还可以看到相应的缓解攻击建议，如图 11-19 所示。

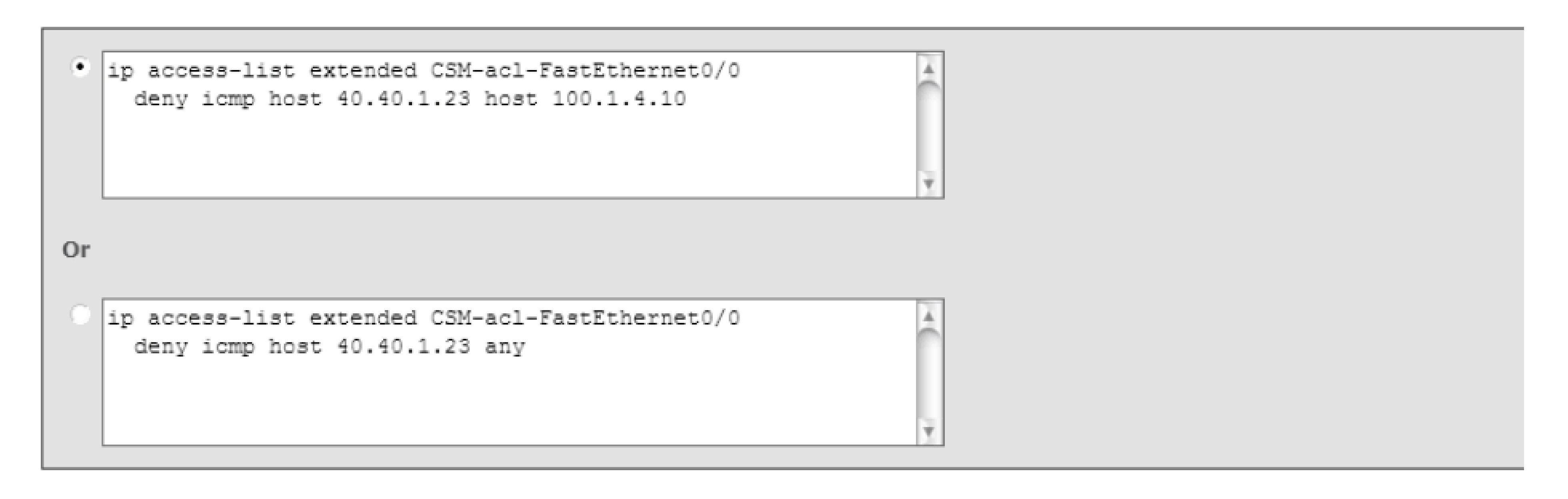


图 11-19　缓解攻击建议

点评与拓展：CS-MARS 是一个非常简单而便捷的网络安全管理系统，它可以方便地添加设备，并自动绘制拓扑图。通过一定时间的学习后，CS-MARS 便可以进行动态的检测，并可以非常智能地给出攻击缓解策略以供管理员选择。

11.2　事件控制系统

除了统一的安全管理软件以外，Cisco 还提供了事件控制系统(Incident Control System，ICS)用于防御病毒、蠕虫等突发事件。ICS 是 Cisco 和 Trend Micro 合作产生的一个产品，TrendLabs 不断监控 Internet，用以发现新的病毒爆发。当 Trend 监控到病毒爆发后，通过相应的威胁分析、快速响应以及其他相关测试确立杀毒方案，并将其转送到 Trend 的自动升级服务器(AU)上，当检测到一个恶意软件爆发后，Trend 同样会开发出一个爆发预防访问控制列表(OPACL)，通常这样的 OPACL 在爆发后 15 分钟就可以发布。此后 Trend 会继续发布一

个预防签名(OPSig)。

Cisco ICS 服务器将自动连接到 AU 服务器，下载 OPACL 和 OPSig，并给相应的 IPS 设备进行特征码升级，同时为 Cisco 交换机和路由器发送 ACL，使得网络设备可以在很短的时间内完成漏洞修复和攻击预防工作。图 11-19 所示是 Cisco ICS 服务器部署示意图。

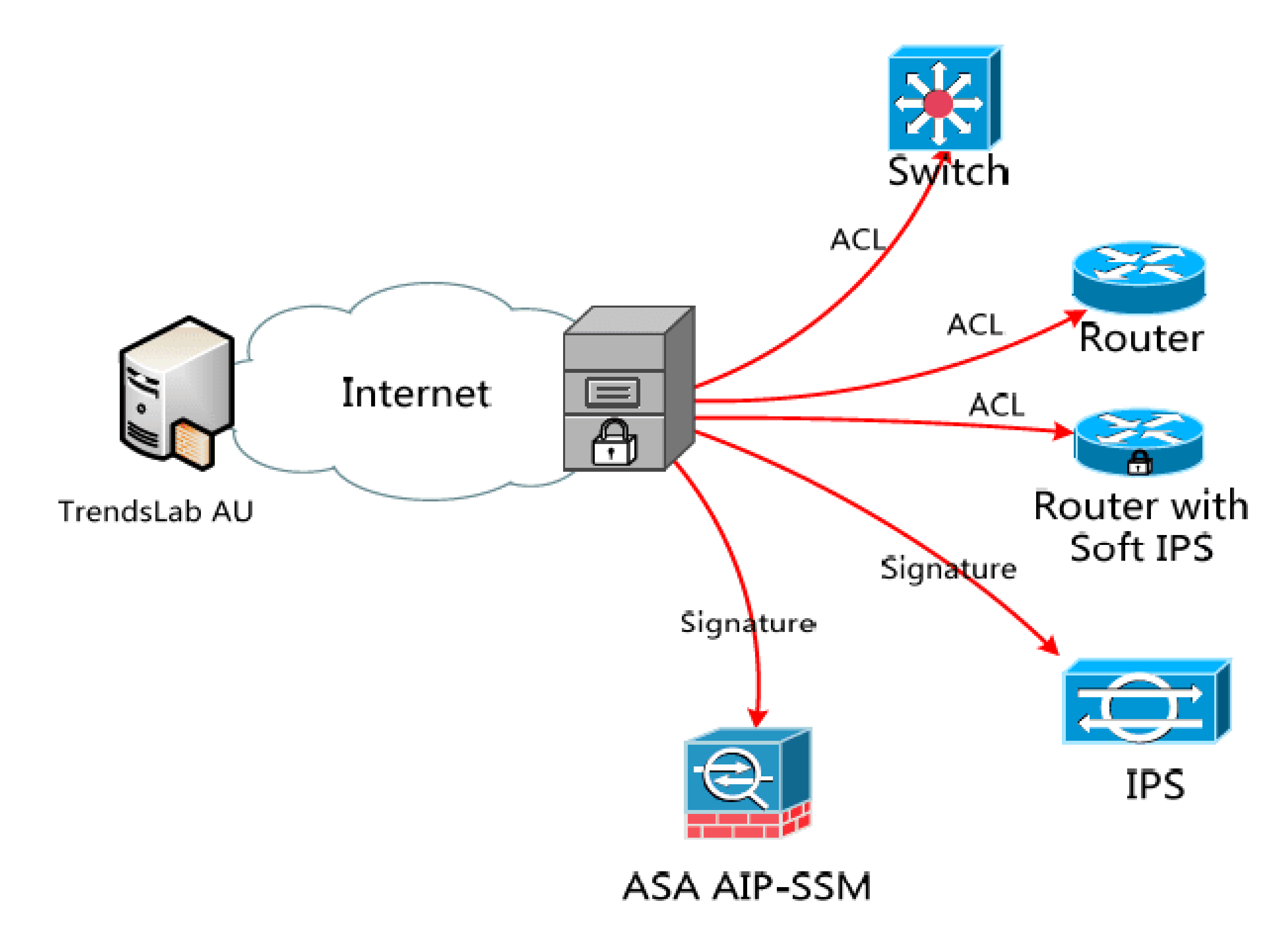


图 11-20　Cisco ICS 服务器部署

11.3 本 章 小 结

本章通过介绍 CS-MARS 和 ICS 提供了一种园区网络统一管理和漏洞快速修复方式。通过部署这样的系统，网络管理员将更加容易应对攻击事情，并通过 CS-MARS 可以快速得到攻击缓解措施，而无须应对大量的日志信息。

第 12 章　文 件 安 全

除了常规网络安全以外，机密文件的加密也是网络安全的一部分。无论网络设备如何的安全，如果文件没有很好地加密，很有可能导致内部盗用，从而威胁整个组织的安全。因此需要对机密文件进行加密，并存放在专门的数据中心中，设置相应的访问权限。

通过本章的学习，读者应掌握以下主要内容：

✧　Windows RMS 服务器的部署

✧　对文件夹使用 EFS 进行加密

12.1　Windows RMS 部署

应用实例导航：Sadness 公司保密文件权限控制

※场景呈现

Sadness 公司需要进行外部审计，要将部分财务数据文件给外部审计人员访问，但是 Sadness 公司数据均使用共享文件服务器存放，如果开放权限，外部审计人员将能够访问很多机密数据，因此财务部人员希望 Jam 能够为他们设计一套安全的文件权限分发系统，Jam 采用了 Windows RMS(权限管理服务，Rights Management Service)来提供权限分发工作。

※技术要领

(1)　RMS 的主要功能；

(2)　RMS 服务器的安装与配置；

(3)　RMS 客户端的安装与配置。

12.1.1　RMS 概述

任何规模的组织都需要保护重要的数字信息，以避免由于疏忽引起误操作以及被恶意利用。此外，信息窃取行为的不断增多以及对保护数据的立法呼声的高涨，使得如何更好地保护数字信息这一需求变得更为强烈。现在，使用计算机来创建和处理以上类型敏感信息的情况越来越多，通过专用网络和公共网络(包括 Internet)扩大连接也日益普及，而计算设备的功能也愈来愈强大，这一切都使得保护组织数据成为必需的安全事项。

数字内容的类型可能包括信息门户中的动态且由数据库驱动的报告、机密的电子邮件、战略计划文档、军事防御报告以及其他敏感的政府文件等。组织会创建和使用各种各样希望保护或必须保护的重要内容。

以下列出了一些可以使用 RMS 来保护的内容。

- ✧ 传统的数字文件和信息。典型的传统数字文件和信息，包括电子邮件通信、与项目有关的文档、机密报告、市场营销计划和产品介绍等。
- ✧ 组织专有信息：高级管理层通过此信息来管理、监控和指导组织的活动，此类专有信息可能包括组织的销售和市场份额报告、财务绩效信息以及战略预测与综述，如果不恰当地分发或使用此类信息，可能会在竞争市场或法律诉讼中给组织带来巨大损失。

部署 RMS 可以作为保护此类敏感信息的安全战略的重要组成部分。

12.1.2 安装与配置 RMS 服务器

RMS 系统建立在 Windows Server 2003 操作系统之上，由服务端和客户端两部分组成。其中，服务端只能安装在 Windows Server 2003 上，不能安装在 Windows Server 2000 或以下版本上。

安装 RMS 首先需要有活动目录支持，其次需要有电子邮件，还需要 MSMQ(消息队列)和数据库支持。下面简要地介绍一下 RMS 服务器的安装与配置过程。

❶ 双击 RMS 安装文件，打开 RMS 安装向导，单击【下一步】按钮。在【许可协议】页面选中【我同意】单选按钮以同意许可协议，并单击【下一步】按钮继续，如图 12-1 所示。

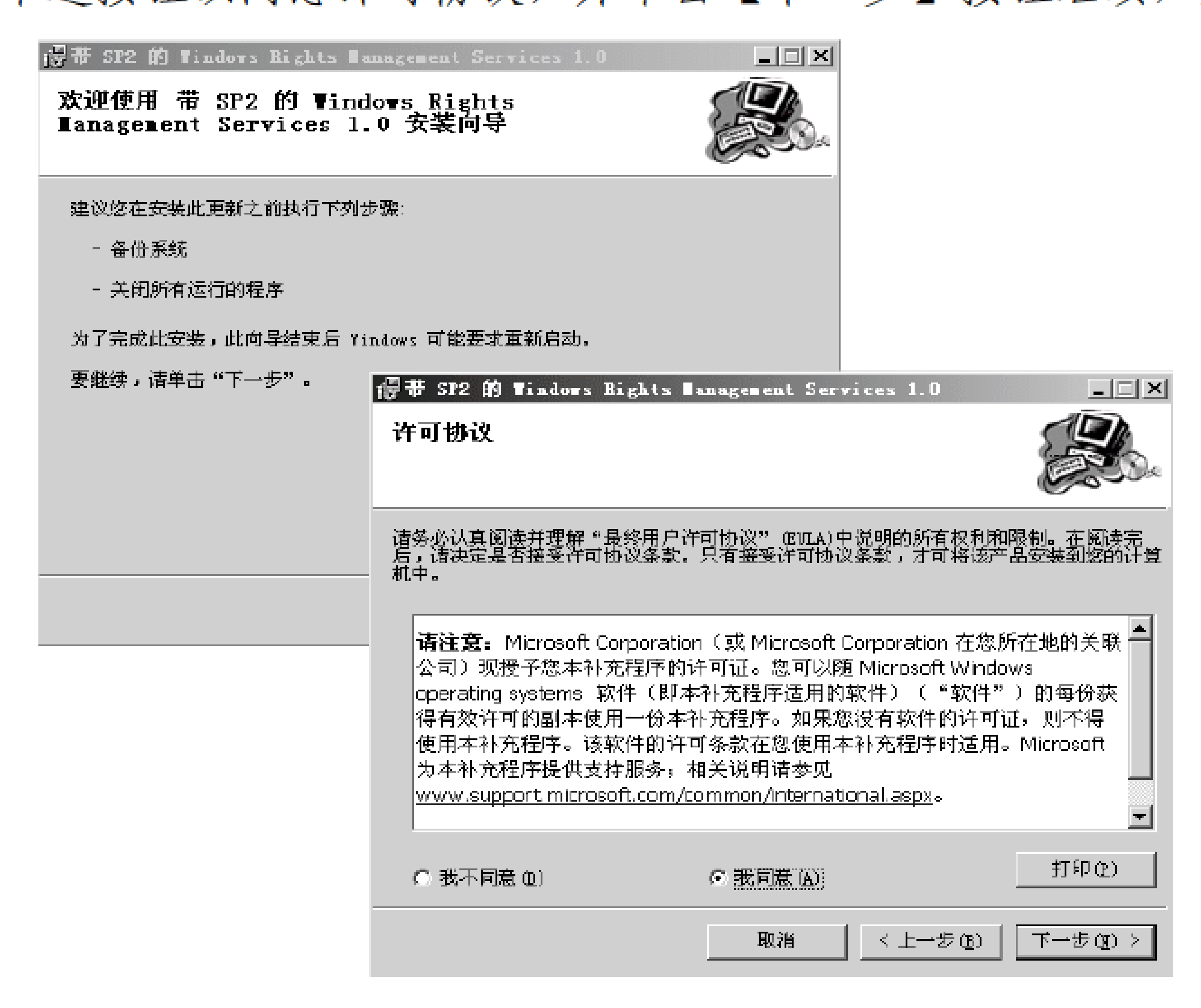


图 12-1　开始安装 RMS

❷ 在【选择安装文件夹】页面中，根据安装的需求选择所安装的文件夹，并单击【下一步】按钮继续，如图 12-2 所示。



图 12-2　选择安装路径

❸ 安装完成后，单击【关闭】按钮，如图 12-3 所示。



图 12-3　完成安装

❹ 依次单击【开始】→【程序】→Windows RMS→【Windows RMS 管理】命令，如图 12-4 所示。

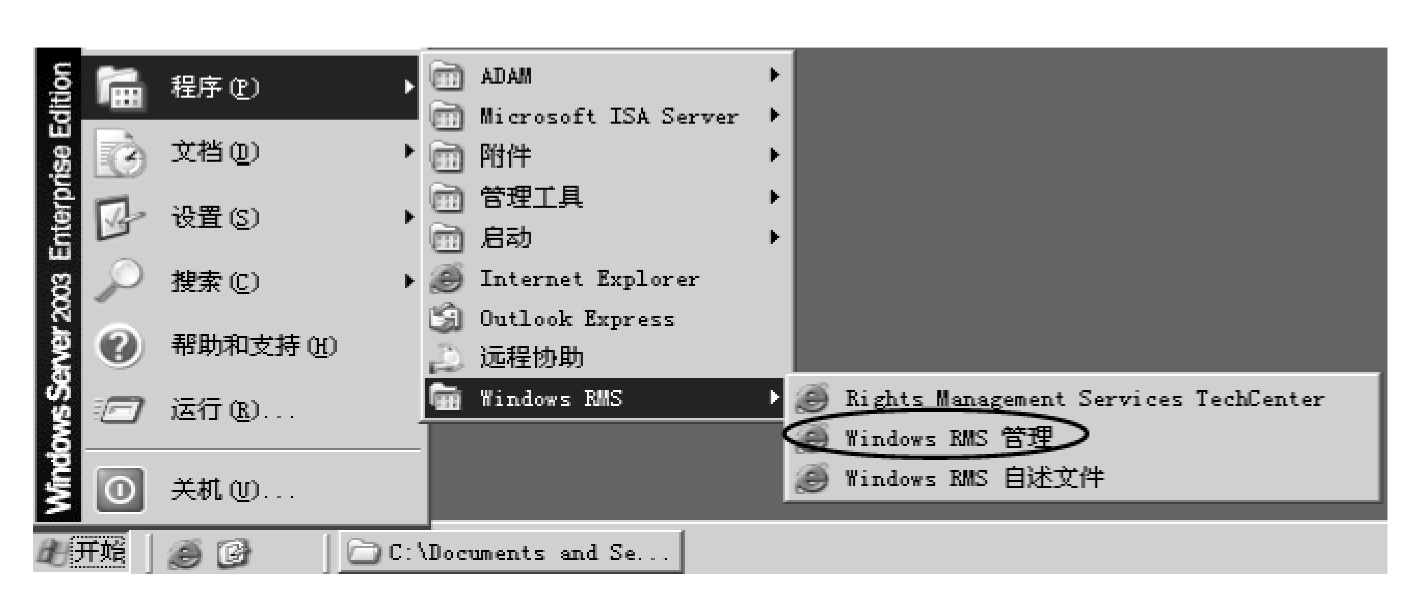


图 12-4　启动 RMS

❺ 在 RMS 全局管理界面中，单击【在此网站上设置 RMS】链接，如图 12-5 所示。

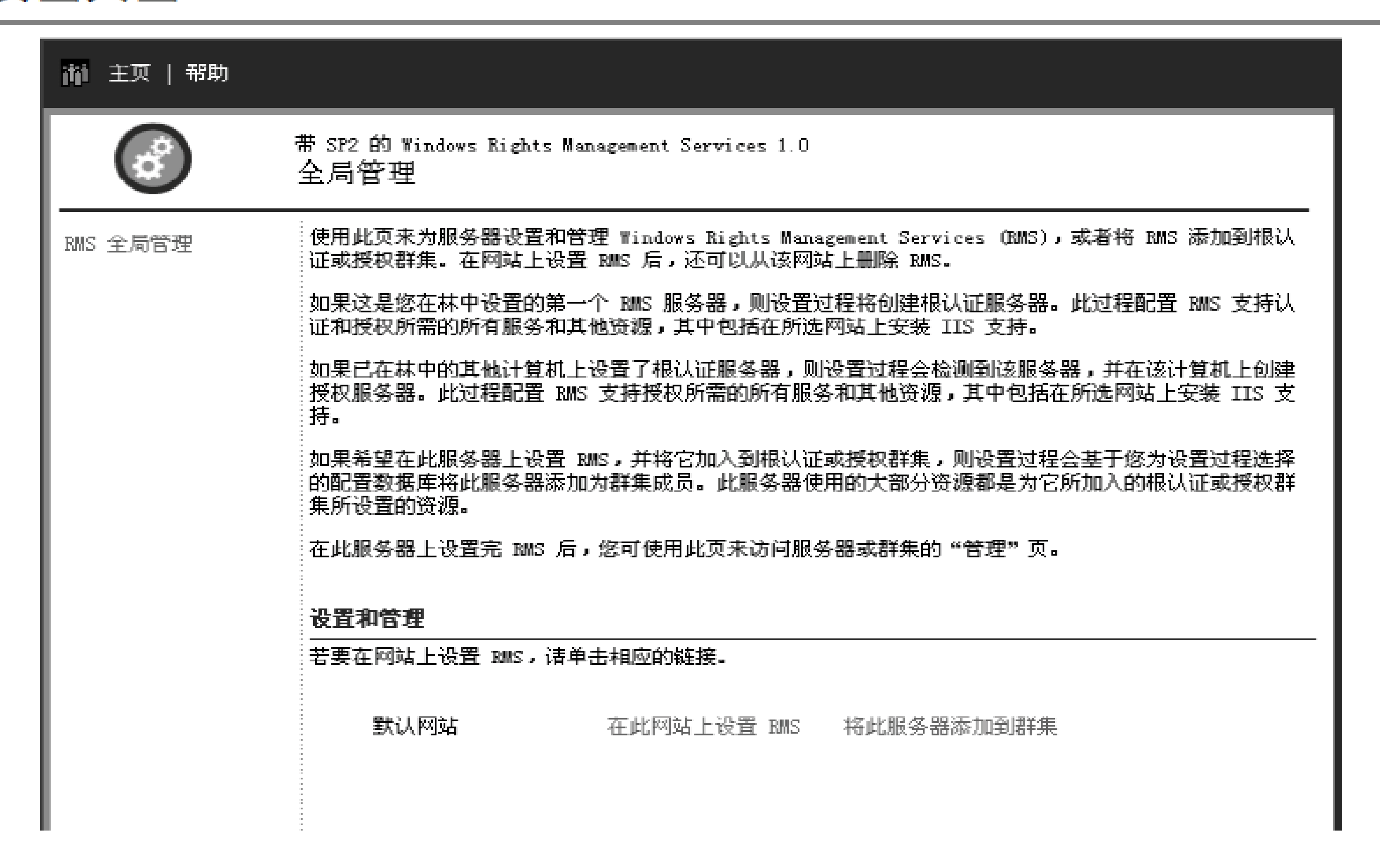


图 12-5　RMS 管理界面

❻ 设置 RMS 根认证服务器。在默认情况下，RMS 会检测 Active Directory 林中是否安装根认证服务器，若没有安装将此服务器将设置为根认证服务器。设置过程为根认证群集设置资源，包括 RMS 使用的数据库，如图 12-6 所示。此后，加入此群集的所有服务器都将使用相同的数据库。

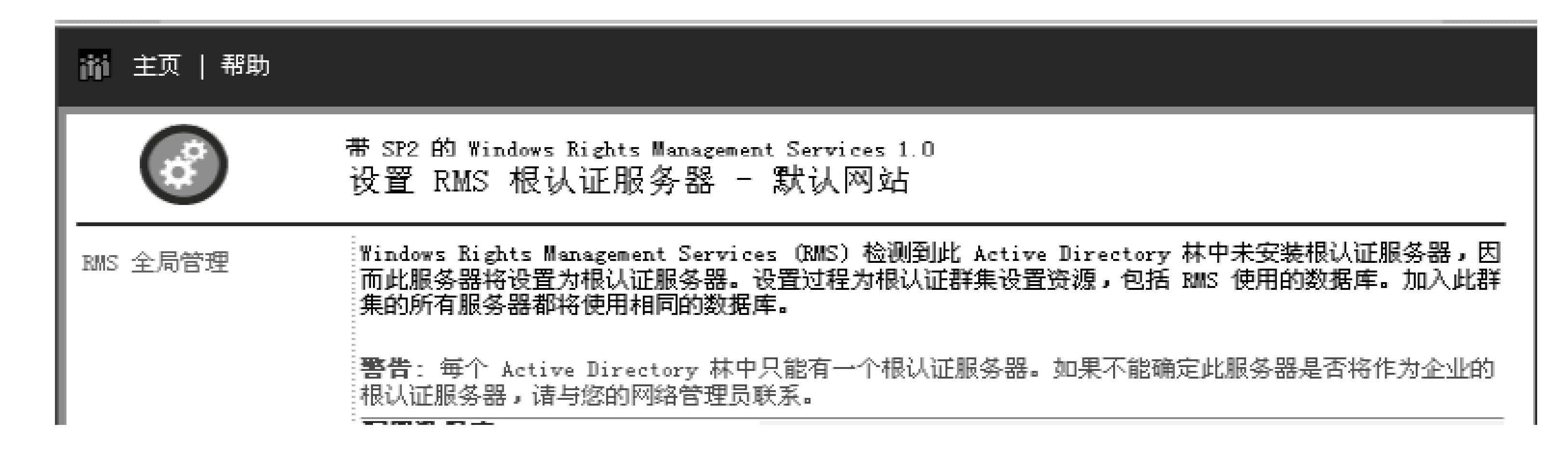


图 12-6　设置 RMS 根认证服务器

❼ 选择 RMS 数据库，如果没有特别需求保持默认设置，如图 12-7 所示。

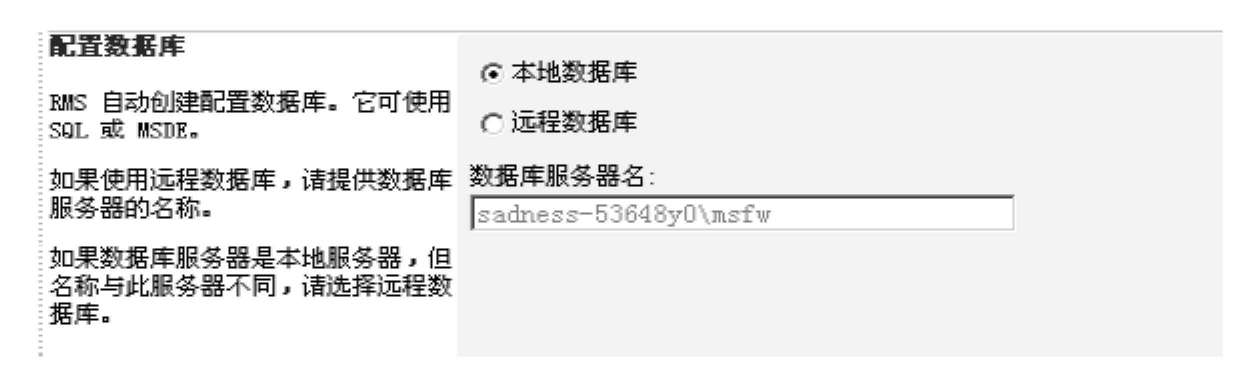


图 12-7　配置 RMS 数据库

❽ 选择 RMS 服务账户，如果没有特别需求保持默认设置，如图 12-8 所示。

❾ 设置群集 URL，如果没有特别需求保持默认设置，如图 12-9 所示。

❿ 设置私钥保护和注册，输入相应的密码，如图 12-10 所示。

⓫ 进行吊销设置后，单击【提交】按钮，如图 12-11 所示。

⓬ 提交后，RMS 将自动向服务器进行注册，如图 12-12 所示。

RMS 服务帐户

指定 RMS 的服务帐户。对于单一服务器安装，您可以选择使用本地系统帐户。对于所有其他安装，则必须指定域帐户。对于域帐户，请提供带有帐户名称的域限定符(例如 DOMAIN\account)。为 RMS 服务帐户指定的域帐户不能与用于安装 RMS 的帐户相同。

警告：本地系统帐户几乎可以访问操作系统上的所有资源，因此会带来严重的安全隐患。如有可能，应避免使用本地系统帐户。

本地系统帐户(仅用于单一计算机安装)

域帐户

用户名：

本地系统帐户

密码：

图 12-8　配置 RMS 服务账户

群集 URL

指定此根认证群集的 URL。它必须注册为企业中的有效 URL。默认情况下，群集 URL 包括此服务器的名称和端口号(如果端口号不为 80)，例如 http://ServerName:8000。

群集 URL：

HTTP:// sadness-53648y0 /_WMCS

图 12-9　设置群集 URL

私钥保护和注册

RMS 为此服务器创建了一个密钥对。选择是使用基于软件的私钥保护方法还是使用基于硬件的加密服务提供程序保护方法来加密配置数据库中的 RMS 私钥。如果使用默认的基于软件的保护方法，请提供一个强密码来加密密钥。

请为服务器许可方证书指定一个名称。默认值是该服务器的名称。

请提供管理员的联系信息(如 RMSAdmin@domain.com)。

使用基于软件的默认私钥保护。

请确保提供一个强密码来在配置数据库中加密 RMS 私钥。

RMS 私钥密码：

再次输入密码：

服务器许可方证书名称：

sadness-53648y0

管理联系人：

图 12-10　设置群集 URL

在某些故障恢复方案或安全方案中，允许第三方吊销根认证群集的服务器许可方证书可能非常有用。此服务器许可方证书总是可以由 Microsoft 吊销。有关 Microsoft 吊销策略的详细信息，请参阅证书实行声明中了解到有关 Microsoft 吊销策略的更多信息。

指定可签署吊销列表以吊销服务器许可方证书的第三方的公钥。

指定可吊销我的企业许可方证书的第三方公钥。

包含可签署吊销列表的公钥的文件：

浏览...

提交

图 12-11　吊销设置



正在此服务器上设置 Windows Rights Management Services，请稍候...

正在设置日志记录。

图 12-12　注册 RMS

⑬ 完成后，单击【返回】按钮回到全局管理界面(如图 12-5 所示)，单击【在此网站上管理 RMS】超链接后将打开【RMS 全局管理】页面，如图 12-13 所示。单击【RMS 全局管理】页面左侧相应的链接即可进入到参数设置管理页面，对某些 RMS 服务参数进行手工配置。其实对于大部分 RMS 服务参数使用默认值即可，除非有特殊的需要，一般不需要手工配置。

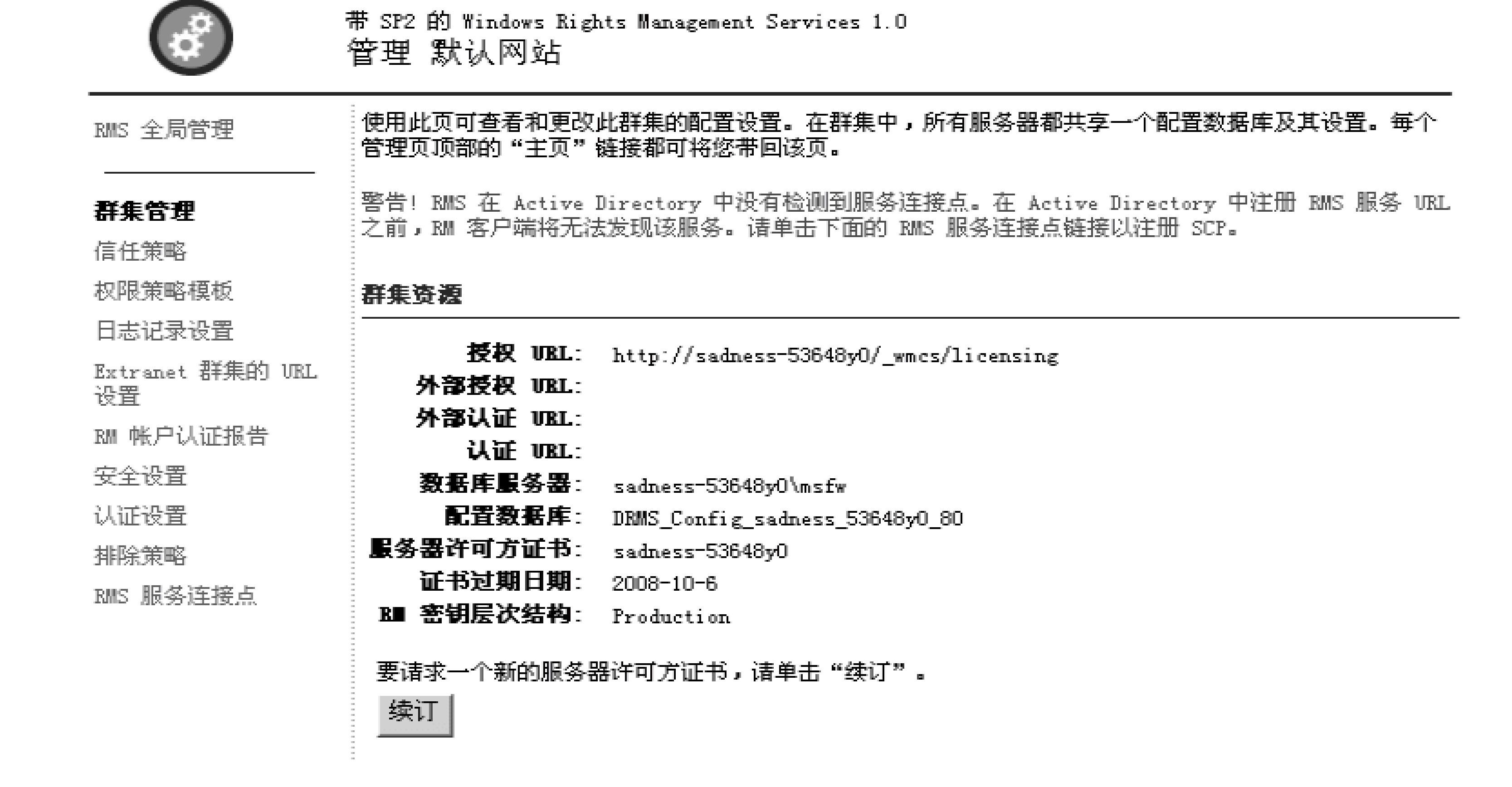


图 12-13　RMS 管理界面

⑭ 单击【RMS 服务连接点】链接，进入设置页，按提示注册 URL，如图 12-14 所示。

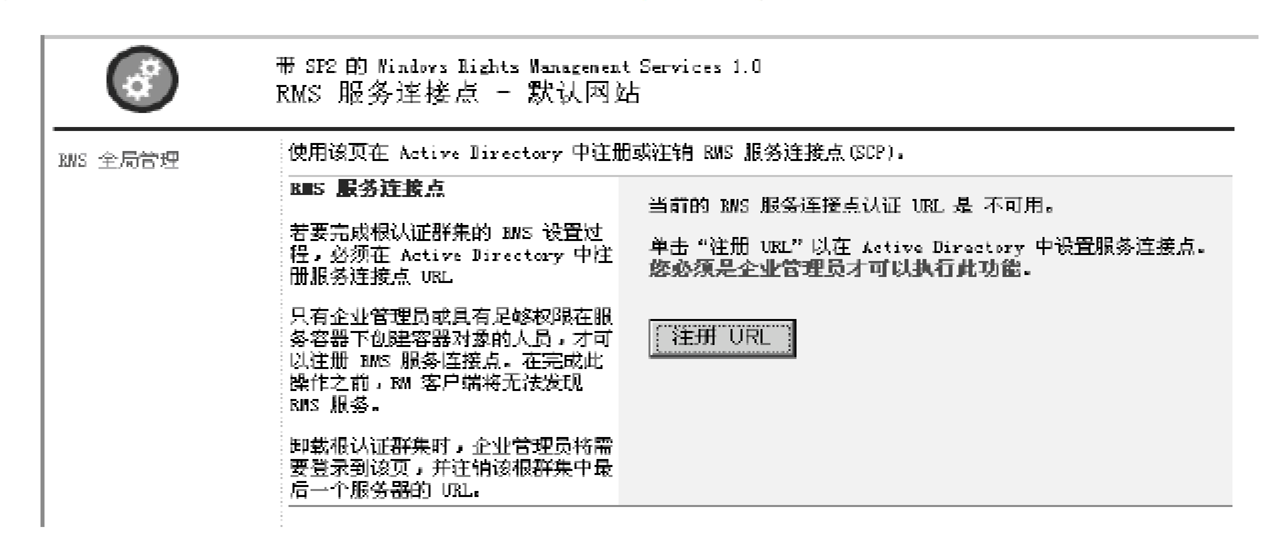


图 12-14　注册 RMS 服务连接点

12.1.3　安装与配置 RMS 客户端

RMS 服务器安装与配置完成后，就可以在进行文件加密的客户机中安装 RMS 客户端软件了。下面简要介绍一下 RMS 客户端的安装与配置过程。

❶ 从 Internet 上按照如下地址下载 RMS 客户端软件。

```
http://www.microsoft.com/downloads/details.aspx?FamilyID=a154648c-881a-41da-8455-042d7033372b&displaylang=zh-cn
```

❷ 在用户计算机上安装 RMS 客户端软件。安装方法很简单，只需依次单击【下一步】按钮即可，如图 12-15 所示。

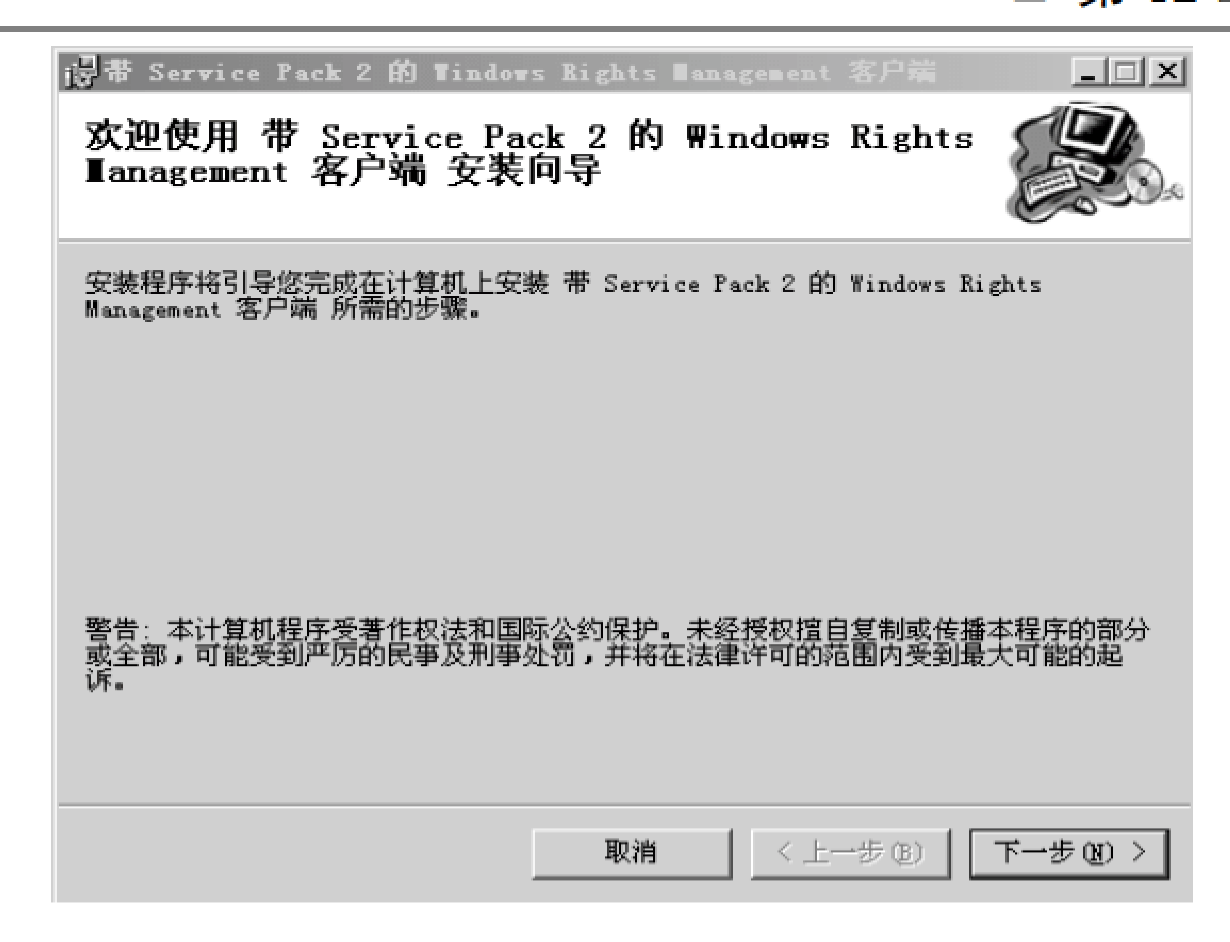


图 12-15　安装 RMS 客户端

❸ 进入 DRM 目录，找到 Actmachine 命令，执行如下命令下载密码箱。

```
actmachine.exe /n /p c:\wrmstemp.cab
```

❹ 将 wrmstemp.cab 解压至 system32 目录下，产生一个 secrep.dll 和一个 secrep.inf 文件，使用如下命令进行安装。

```
rundll32.exe advpack.dll, LaunchINFSection secrep.inf, Install,, N
```

❺ 启动 Microsoft Office 等支持 RMS 的软件，选择某个文档进行 RMS 设置。例如，要对某一 Word 文档进行 RMS 设置，可以单击工具栏中 图标，便弹出了如图 12-16 所示的对话框。

❻ 在【权限】对话框中，根据实际需要设置文档的权限，如图 12-17 所示。

点评与拓展： RMS 是一种简单而又安全的文件权限设置工具，为了扩大 RMS 服务的应用范围现在微软正在积极与一些软件开发商、系统集成商合作以开发出更多的支持 RMS 服务的应用程序产品。RMS 配合 EFS 文件加密系统可以进行数据安全保护。

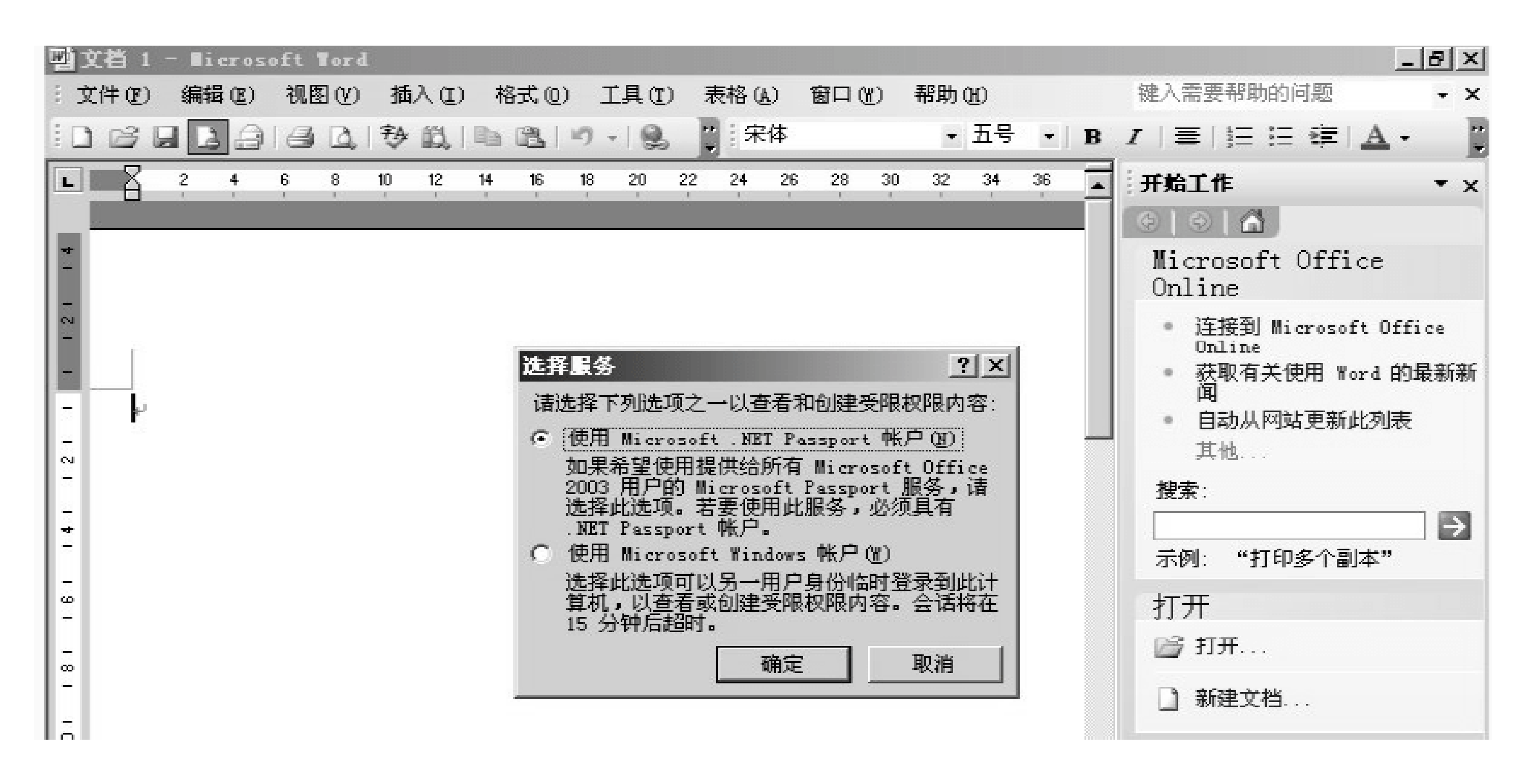


图 12-16　设置 RMS

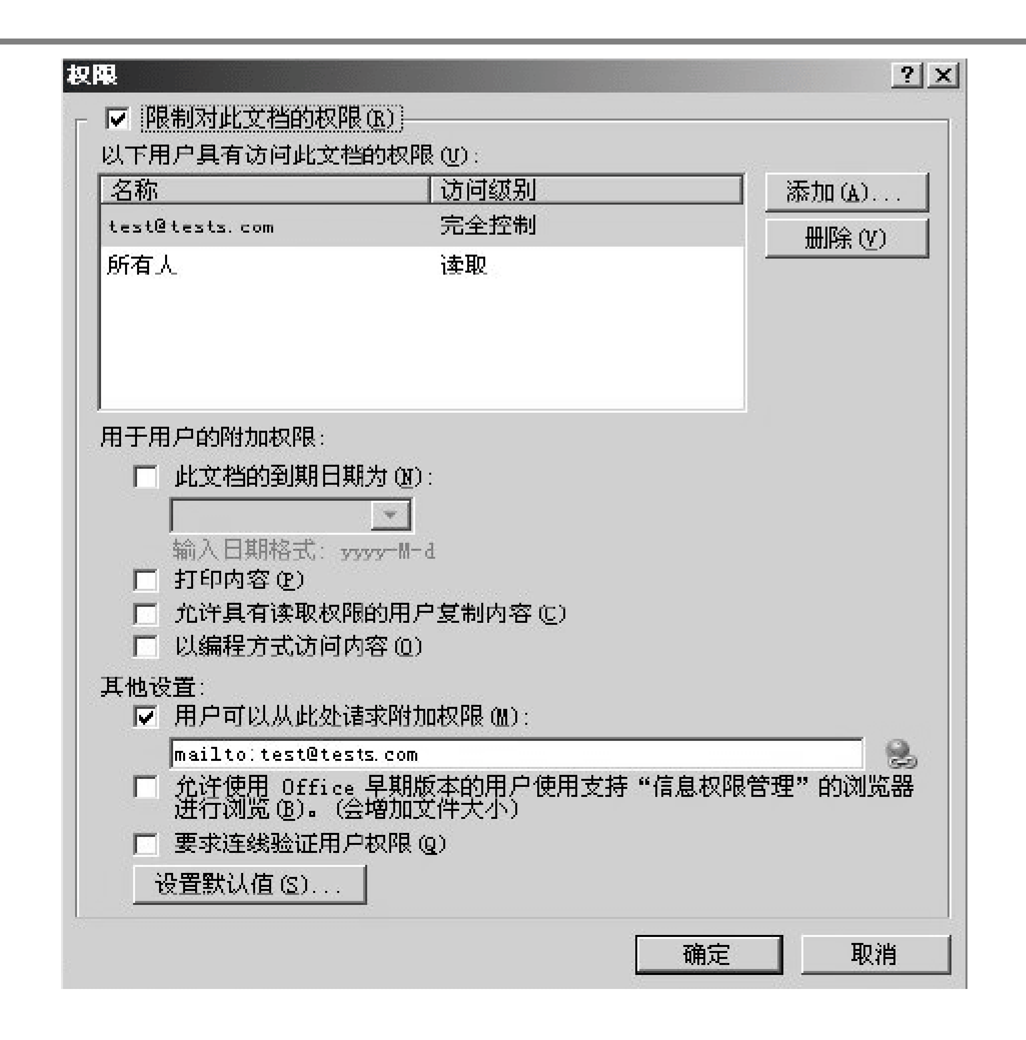


图 12-17　设置 RMS 权限

12.2　EFS　加　密

加密文件系统 (EFS) 是 Windows 2000、Windows XP Professional (Windows XP Home 不包含 EFS)和 Windows Server 2003 的 NTFS 文件系统的一个组件，它采用高级的标准加密算法实现透明的文件加密和解密。任何不拥有合适密钥的个人或者程序都不能读取加密数据，即便是物理拥有保存加密文件的计算机，加密文件仍然受到保护；甚至是有权访问计算机及其文件系统的用户，也无法读取这些数据。

下面是对文件进行加密的操作步骤。

❶ 选定需要进行 EFS 加密的文件夹，右击，在弹出的快捷菜单中选择【属性】命令，弹出文件夹的【属性】对话框，单击【高级】按钮，如图 12-18 所示。

❷ 在文件的【高级属性】对话框中，选中【加密内容以便保护数据】复选框，然后单击【确定】，如图 12-19 所示。



图 12-18　使用 EFS 加密

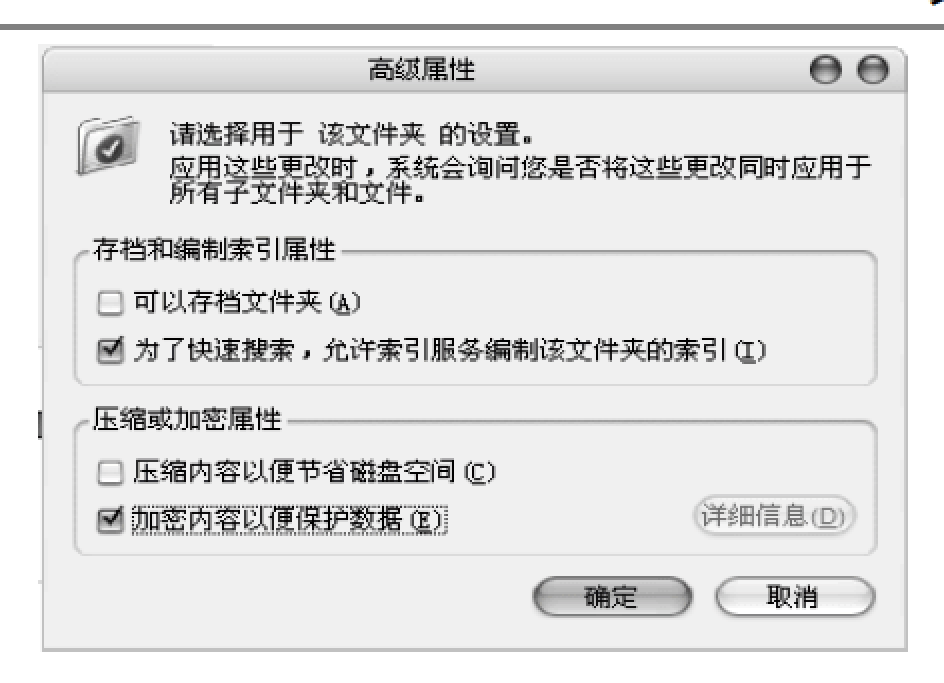


图 12-19　选中【加密内容以便保护数据】复选框

❸ 在【确认属性更改】对话框中，若选中【仅将更改应用于该文件夹】单选按钮，系统将只将文件夹加密，里面的内容并没经过加密，但是以后在其中创建的文件或文件夹将被加密；若选中【将更改应用于该文件夹、子文件夹和文件】单选按钮，文件夹内部的所有内容被加密，如图 12-20 所示。

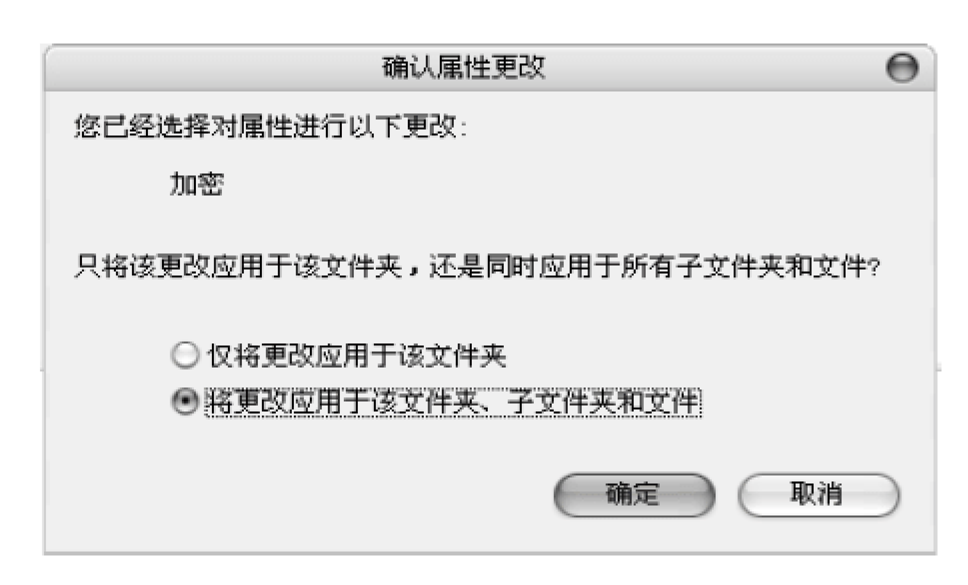


图 12-20　选择应用加密更改的文件范围

❹ 单击【确定】按钮，就完成了文件夹的 EFS 加密操作。此时，文件夹颜色会发生改变，表示 EFS 加密操作成功。

12.3　本 章 小 结

本章介绍了基于微软 RMS 的文件权限管理系统，同时也介绍了使用 EFS 进行文件加密的配置过程。文件加密和权限控制也是园区网络安全中非常重要的一环，对于数据中心，可以使用其他更加严格的加密方式进行加密处理。

第 13 章　园区网络安全设计

通过前面 12 章的学习，我们了解了实现网络安全的一些策略和方法，而如何有效地将这些策略结合起来，设计一个安全的园区网络成为我们必须讨论的话题。网络安全也遵从“木桶理论”(一个木桶能盛多少水取决于最短的那块木板有多长)，网络安全中最薄弱的一环决定了整个网络的安全状况，因此网络安全并不是简单地添加一个防火墙或者一个入侵检测系统，网络安全是一个整体，需要每个环节的提升。

通过本章的学习，读者应掌握以下主要内容：

✧　小型企业网络安全设计
✧　中型企业网络安全设计
✧　大型企业网络安全设计
✧　校园网络安全设计
✧　运营商网络安全设计

13.1　小型企业网络安全设计

应用实例导航：小型企业 SAAA 网络安全解决方案

※场景呈现

SAAA 是一家刚起步的小型企业，企业的网络规模不大，用于网络安全建设的费用相对较少，因此设计网络安全方案的时候，需要综合价格和安全性等因素进行考虑。SAAA 创立初期的网络拓扑结构如图 13-1 所示。

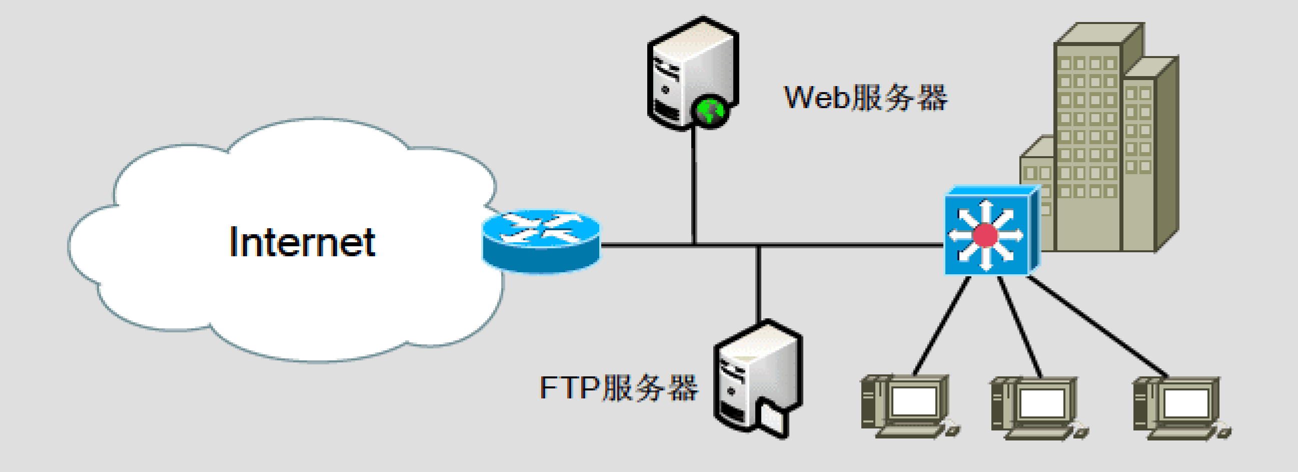


图 13-1　小型企业网络

※设备清单

(1)　路由器：仅支持 NAT 等简单功能以及仅支持 RIP 协议的小型企业路由器；

(2) 交换机：多台普通 24 口交换机，不支持 VLAN 等功能；
(3) 服务器：基于微软 IIS 的 Web 服务器和 FTP 服务器，未作任何相关的安全配置；
(4) 办公用机：50 ～100 台普通台式机或者笔记本，未安装杀毒软件或长期没有更新；
(5) 无线 AP：没有任何加密措施。

如应用实例中的小型企业网络在我国十分常见，通常这类企业在刚起步的阶段并没有足够的精力投入到网络建设上来。其内网环境与大多数网吧一样，组网方式随意性很强，安全防护手段部署原则不明确；网段间的边界不清晰，并且网段间的控制较差，通常为了能够访问，将内网中很多机器允许外网访问；对于病毒等防御措施不够，攻击容易扩散，并且在攻击爆发后，没有缓冲处理时间；虽然有些企业购买了防火墙等安全设备，但错误的配置却无法发挥作用。

设计一个安全的园区网络，通常按照如图 13-2 所示的区域对网络进行划分，然后根据企业的发展阶段添置相应的区域。例如，小型企业的网络规模较小，并不需要专用的管理区域，同时可能由于资金有限，仅需要简单的 VPN 服务。

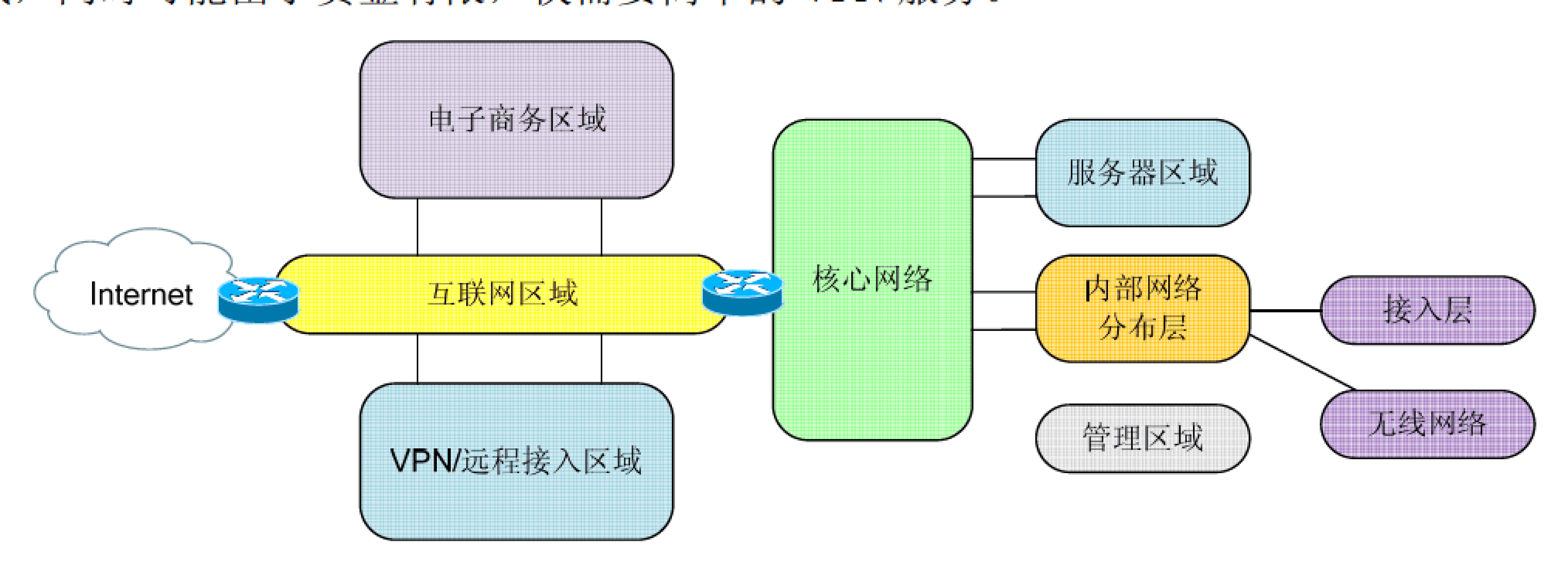


图 13-2　安全园区网络区域划分

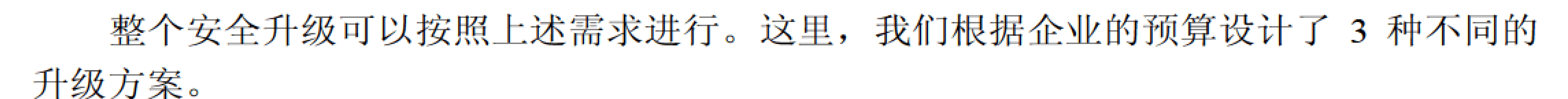
在进行网络安全升级的时候，首先需要做的就是对公司安全现状的了解，并对安全状况进行审计，确定需要升级的环节。

例如，对前文所述的某小企业进行安全审计的结果如下。

- ✧ 网络没有明显的区域划分；
- ✧ 网络中没有任何安全设备；
- ✧ Web 服务器和 FTP 服务器没有安全保护；
- ✧ 办公杀毒软件和系统补丁升级不及时导致非常容易受到攻击；
- ✧ 无线网没有加密。

应对这些情况，需要进行升级的项目如下。

- ✧ 配置 WSUS 服务器，确保系统补丁能够快速安装；
- ✧ 每台机器使用杀毒软件需及时更新；
- ✧ 购置防火墙等设备，确保关键服务器安全；
- ✧ 无线网络采用加密的方式进行接入；
- ✧ 企业网络需要进行较为明显的区域划分。



整个安全升级可以按照上述需求进行。这里，我们根据企业的预算设计了 3 种不同的升级方案。

1. 廉价升级方案

很多小型企业已经购置了 Windows 2003 企业版系统，因此可以先基于 Windows 2003 系统的一些服务进行安全改造。

- ✧ WSUS 服务：使系统安全补丁能够快速分发；
- ✧ 活动目录、证书服务：方便企业管理，并为企业后续发展提供一个好的基础；
- ✧ RMS 服务：方便文件权限管理；
- ✧ Radius 服务：为用户接入提供身份认证。

防火墙及 VPN 可以选择使用基于 Linux 的解决方案，并且还可以配置基于 Linux Snort 的 IDS 方案，同时设置两台 IDS 分别监控服务器区域和办公区域。对于无线网络，需要使用提供加密接入的无线路由器或无线 AP，一些 SOHU 级的无线路由器即可满足廉价型升级方案的需求，例如 Linksys WRT54G。同时可以在这类路由器上安装第三方的固件使其拥有功率控制功能，有效防止公司外部的非法侦听。

杀毒软件可以选择 Norton 或者 Trend Micro 企业版杀毒软件，但是我们建议选择趋势的企业版杀毒系统，因为随着公司规模的不断扩大，以后使用 ASA、NAC 等技术的时候，可以充分利用趋势企业版杀毒软件。

前端路由器可以选择 Linksys RV402，它不但提供双线路接入功能，还可以提供简单的防火墙和 VPN 接入功能，售价也非常便宜。

小型企业廉价升级方案所需要设备清单如表 13-1 所示。

表 13-1　小型企业网络廉价升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux IDS 服务器	2
	Linux 防火墙服务器	1
	Windows/Linux Radius 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
杀毒软件	Norton/Trend Micro SOH 企业版杀毒软件	1
路由器	Linksys RV402	1

实施廉价升级方案后的网络拓扑如图 13-3 所示。

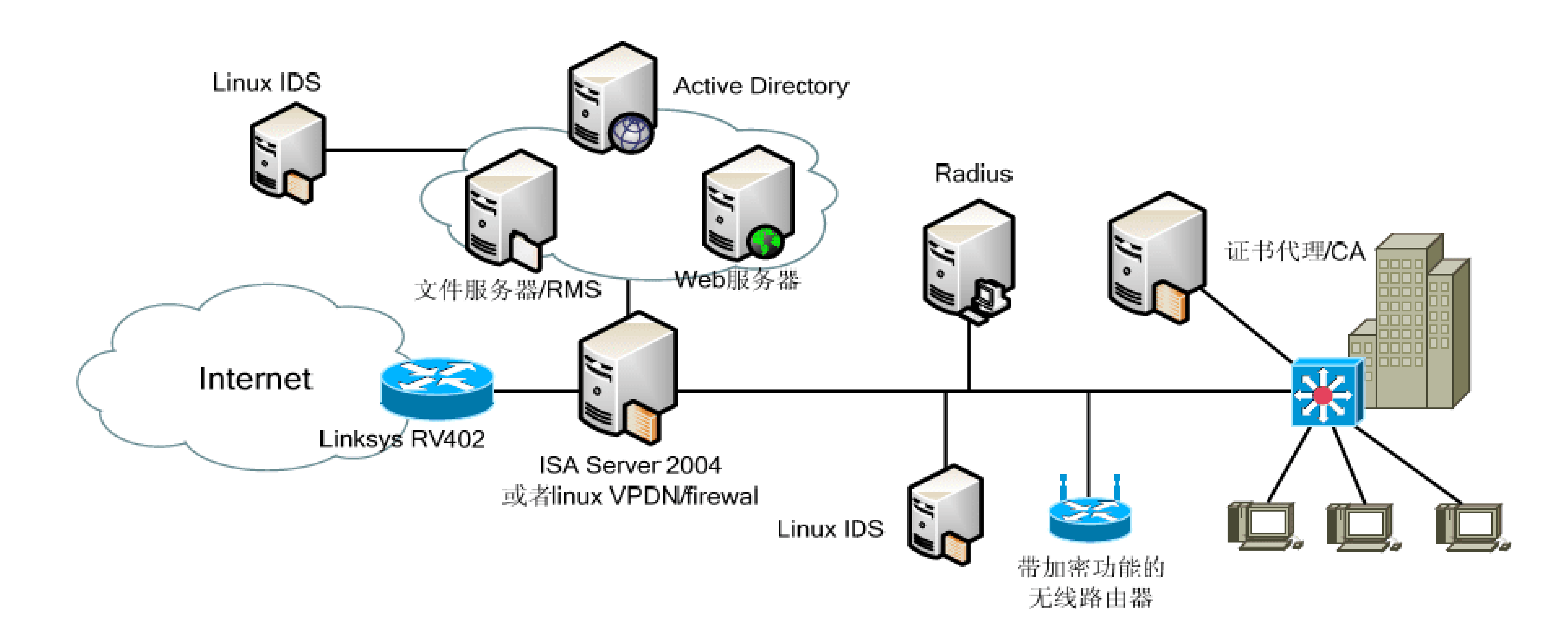


图 13-3　小型企业网络廉价升级方案

2. 高性价比升级方案

对于主要是电子、通信、软件等行业的用户，它们通常需要更加安全的网络来保护企业的程序、代码等。但是很多企业面对激烈的竞争，不可能提供很多经费用于这样的升级，因此他们是小企业高性价比升级方案的使用者，通常这类方案在廉价方案的基础上更换了更加安全的防火墙产品，并且严格控制客户端的接入，防止内网病毒导致的数据丢失等，这类网络需要更加明确的区域划分。

在廉价方案的基础上，我们建议将连接 Internet 的路由器更换成 Cisco ISR 1800 系列集成多业务路由器，不但集成了基于 IOS 的防火墙、访问控制等功能，还提供了 NAC 接入访问控制和无线 AP 功能，同时为以后公司业务升级、创建异地办公室提供了 VPN 支持和语音支持。在 Cisco ISR 1841 上还可以配置集成的 IPS 模块，更加有效地检测入侵行为，保护网络安全，如图 13-4 所示。



图 13-4　ISR 集成入侵防御模块

同时，我们建议使用 Cisco Catalyst 3560 或者 3750 系列交换机用于提供 PVLAN、DHCP SNOOping、动态 VLAN、ARP 病毒防护等机制，实现基本的网络安全，同时由于提供了 VLAN 功能，还可以更加清晰地划分网络的业务区域。若全网均采用 Cisco 设备，可以非常廉价地实现基于 NAC Framework 的接入访问控制服务。与此同时，使用 Radius 服务器对路由器和交换机配置 AAA 控制。

小型企业网络高性价比升级方案所需设备清单如表 13-2 所示。

表 13-2 小型企业网络高性价比升级方案设备清单

名 称	描 述	数 量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 1841	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Norton/Trend Micro 企业版杀毒软件	1

实施高性价比升级方案后的网络拓扑如图 13-5 所示。

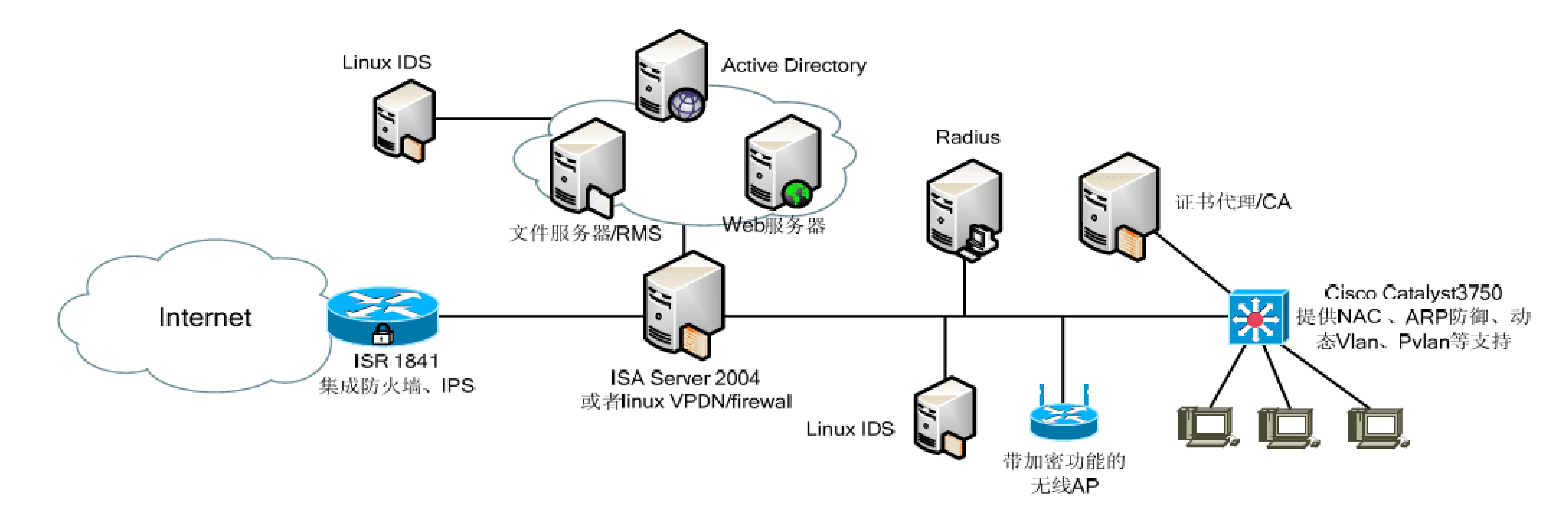


图 13-5 小型企业网络高性价比升级方案

3. 高安全性升级方案

对于资金较为充裕的小型企业可以使用 ASA 5505(如图 13-6 所示)，实现 UTM 统一管理威胁，并替换原有的 Linux Firewall/ISA Server。



图 13-6 ASA 5505

基于模块化的接口可以像更高系列的 ASA 一样扩展接口，内置 8 个 POE 以太网供电接

口，可以有效地支持 IP 电话等设备。对于资金充足的用户，还可以选择 2 台 ASA 进行失效转移配置，可以购置防病毒模块与已有的 Trend Micro 杀毒软件进行联动。网络高安全性升级方案所需设备清单如表 13-3 所示。

表 13-3　中小企业网络高安全性升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux IDS	2
	Cisco Secure ACS 服务器	1
UTM	Cisco ASA 5005	2
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 1841	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Norton/Trend Micro 企业版杀毒软件	1

实施高安全性升级方案后的网络拓扑如图 13-7 所示。

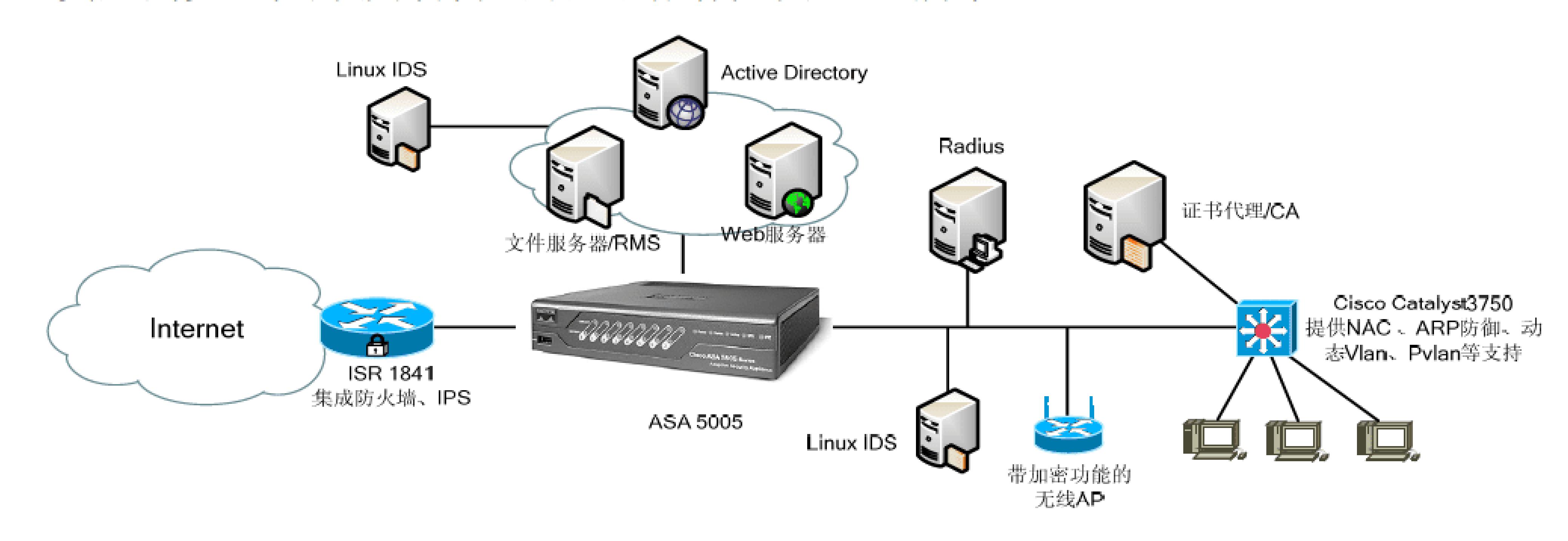


图 13-7　小型企业网络高安全性升级方案

13.2　中型企业网络安全设计

应用实例导航：中型企业 EDGE-EA 网络安全解决方案

※场景呈现

EDGE-EA 是通信行业的一个中型企业，拥有数千名员工，并且在全国各地设立了分支

机构，他们的销售人员通常在进行销售的过程中，需要使用一种安全的方式和总部联系来确定订单价格，或给客户演示产品使用环境等，对 VPN 的需求较高。

为了有效保护自己的研发资料不被恶意攻击，这家企业较为注重网络安全，在其发展的过程中已经购置了一些网络安全设备，但由于网络区域划分不科学，这些设备通常没有发挥很大的作用。由于经费问题，使用的防火墙并不能在透明模式下工作，遇到攻击后，防火墙一旦损坏就会导致网络中断。同时，这家企业重视总部网络安全，忽视分支机构网络的安全。如图 13-8 所示的是 EDGE-EA 公司的网络拓扑结构示意图。

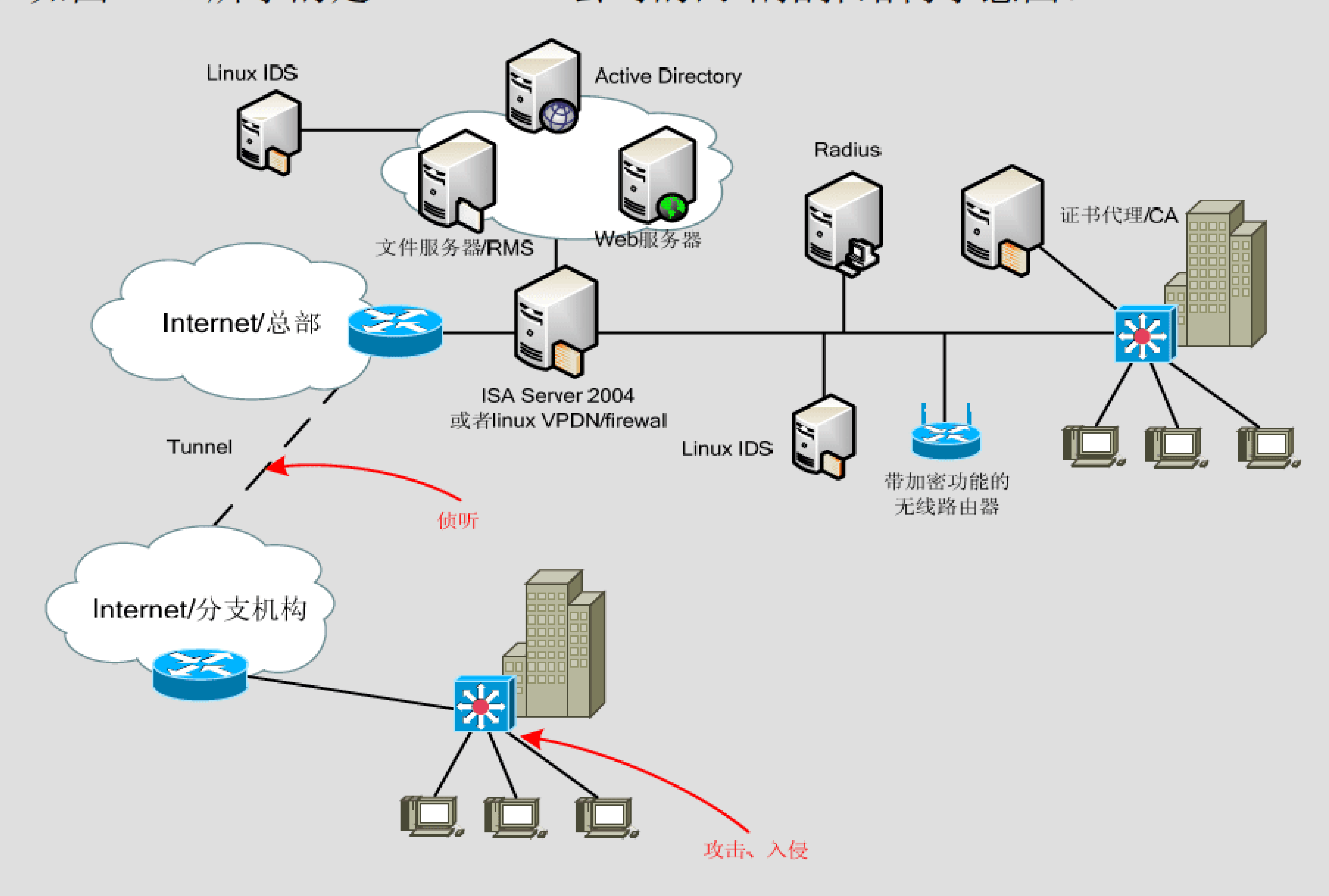


图 13-8　中型企业网络

某信息安全风险评估机构对 EDGE-EA 公司进行安全审计，其结果如下。

- ✧ 分支机构和总部的连接需要采用更安全的 IPSec VPN 或者 MPLS VPN；
- ✧ 为经常出差的用户提供 VPDN 或者 SSL VPN；
- ✧ 网络中接入的主机需要更加严格的接入控制；
- ✧ 杀毒软件需要进行集中的更新管理；
- ✧ AD、CA、RMS、Radius 等服务器需要进行冗余配置；
- ✧ 总部防火墙需要进行冗余配置；
- ✧ 核心网络路由协议需要进行严格的加密；
- ✧ 核心网络需要进行冗余配置；
- ✧ 所有的网络设备需要配置 AAA 认证；
- ✧ 交换机需要进行安全保护，并配置热冗余备份；
- ✧ 防火墙应当支持透明模式。

在网络安全性升级设计时，分支机构可以参考上一节的小型企业配置，AD、CA 等基于 Windows 的服务器均可以配置成每个分支机构一套这样的服务器，在总部配置 AD、CA

的根服务器。同时可以根据实际的情况选择 ASA5510～ASA5550 部署在网络前端，实现防火墙、VPN、IPS 和防病毒网关功能。同时，由于员工数量较多，可以在内部网络中实现 CSA-MC 统一管理客户端安全，防止病毒大规模爆发的损失。

由于这类企业通常在发展过程中，网络经历了多次升级，因此网络中的设备经常来自很多不同的厂商，为了保持兼容性，我们建议使用 NAC Appliance 接入控制，防止带病毒主机连入网络。同时还可以使用 CSA-MC 和 IPS 进行联动，使得网络更加安全。

1. 廉价升级方案

中型企业分支机构和小型企业的廉价升级方案类似，设备清单如表 13-4 所示。

表 13-4　中型企业分支机构网络廉价升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux IDS 服务器	2
	Linux 防火墙服务器	1
	Windows/Linux Radius 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
杀毒软件	Trend Micro 企业版杀毒软件	1
路由器	Linksys RV402	1(提供到总部的 IPSec 连接)

分支机构实施廉价升级方案后的拓扑结构如图 13-9 所示。

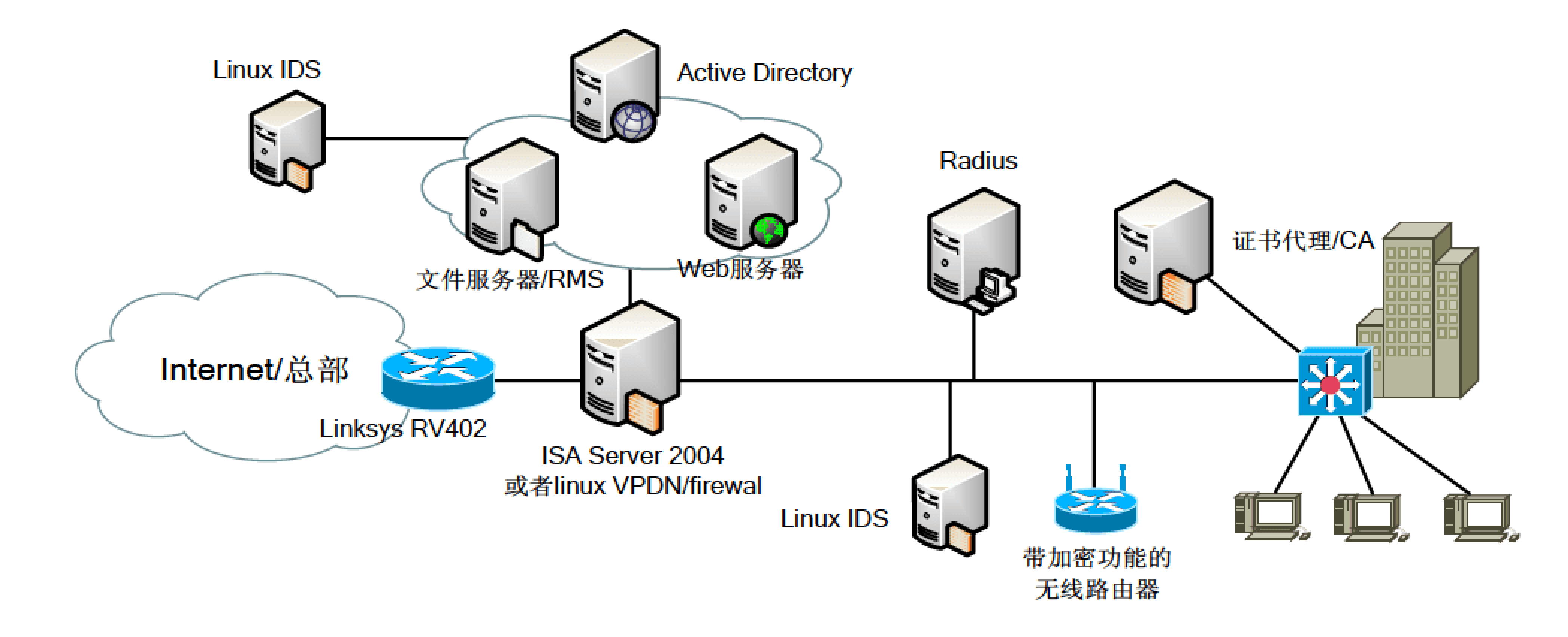


图 13-9　中型企业分支机构网络廉价升级方案

企业总部由于员工较多，并且需要多个远程分支机构连接，因此前端路由器选择了基于 ISR 2800 系列的路由器，并且在公司总部网络安装 Trend Micro 管理中心，用于管理分

支机构网络的 Trend Micro 企业版杀毒软件。同时配置 WSUS、CA、AD 为根服务器，并为总部配置基于 NAC Framework 的访问控制。中型企业总部网络廉价升级方案所需设备清单如表 13-5 所示。

表 13-5　中型企业总部网络廉价升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器(根服务器)	1
	CA 服务器(根服务器)	1
	AD 服务器(根服务器)	1
	RMS 服务器(根服务器)	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 2800	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Trend Micro 企业版杀毒软件	1
	Trend Micro 管理中心	1
NAC	NAC Framework	1

实施网络廉价升级方案后的网络拓扑如图 13-10 所示。

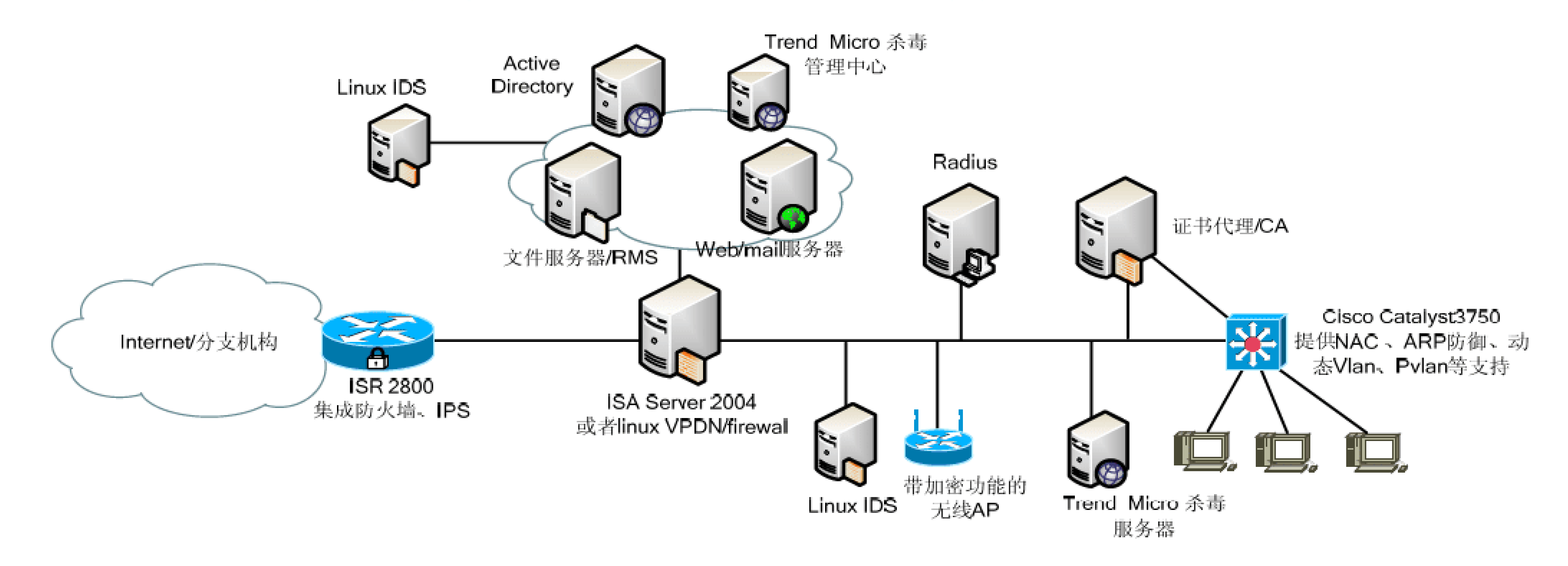


图 13-10　中型企业总部网络廉价升级方案

2. 高性价比升级方案

在高性价比升级方案中，我们可以考虑增加部署基于 CSA 的客户端行为保护系统。中

型企业分支机构和小型企业的高性价比升级方案类似，设备清单如表 13-6 所示。

表 13-6　中型企业分支机构网络高性价比升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 1841	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Norton/Trend Micro　企业版杀毒软件	1
客户端安全	CSA	为每台电脑配置
	CSA-MC	1

实施高性价比安全升级方案后的拓扑结构如图 13-12 所示。

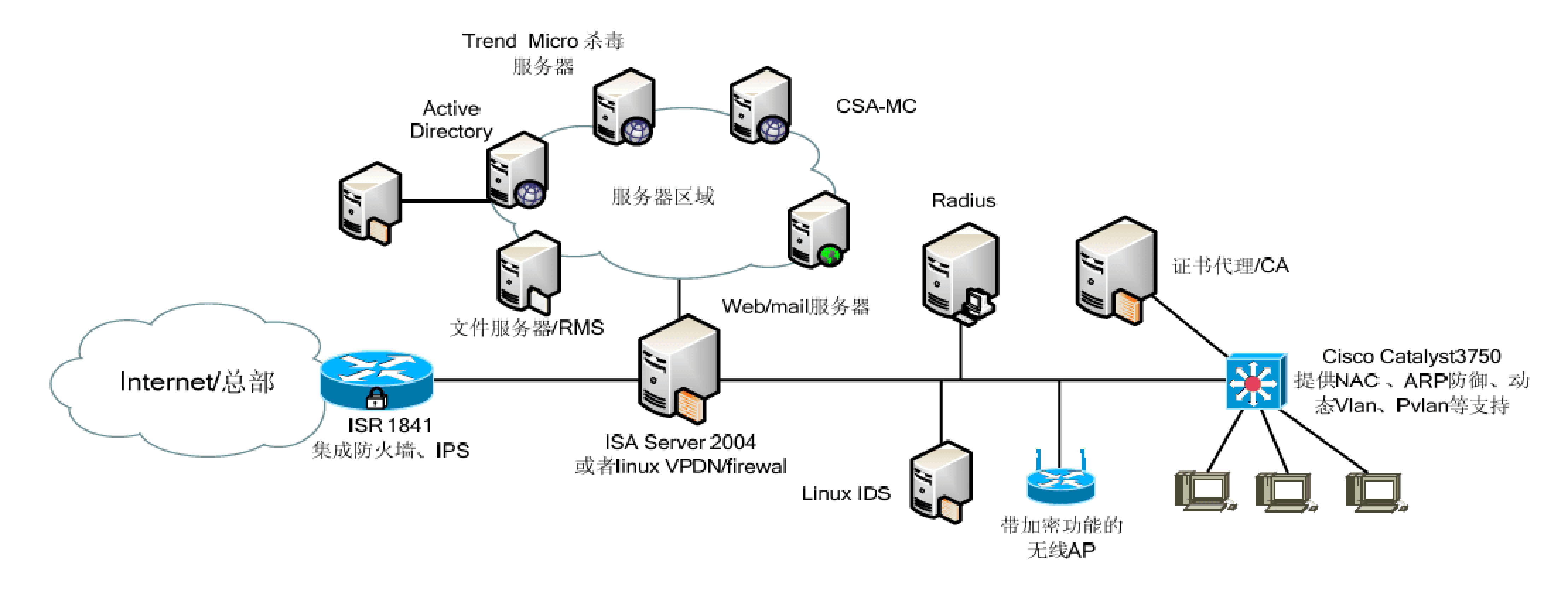


图 13-11　中型企业分支机构网络高性价比升级方案

对于企业总部，可以选择使用 ISR 3800 路由器获得更好的性能，同时在总部尽量使用统一厂商的设备，提供整体性的安全解决方案。例如基于 Cisco 的 NAC Framework、CSA-MC 和 IPS 系统进行联动等，确保获得更高的安全性能。中型企业总部网络高性价比升级方案所需设备清单如表 13-7 所示。

表 13-7　中型企业总部网络高性价比升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器(根服务器)	1
	CA 服务器(根服务器)	1
	AD 服务器(根服务器)	1
	RMS 服务器(根服务器)	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 3800	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Trend Micro　企业版杀毒软件	1
	Trend Micro 管理中心	1
NAC	NAC Framework	1
客户端安全	CSA	为每台电脑配置
	CSA-MC	1

实施高性价比安全升级方案后的拓扑结构如图 13-12 所示。

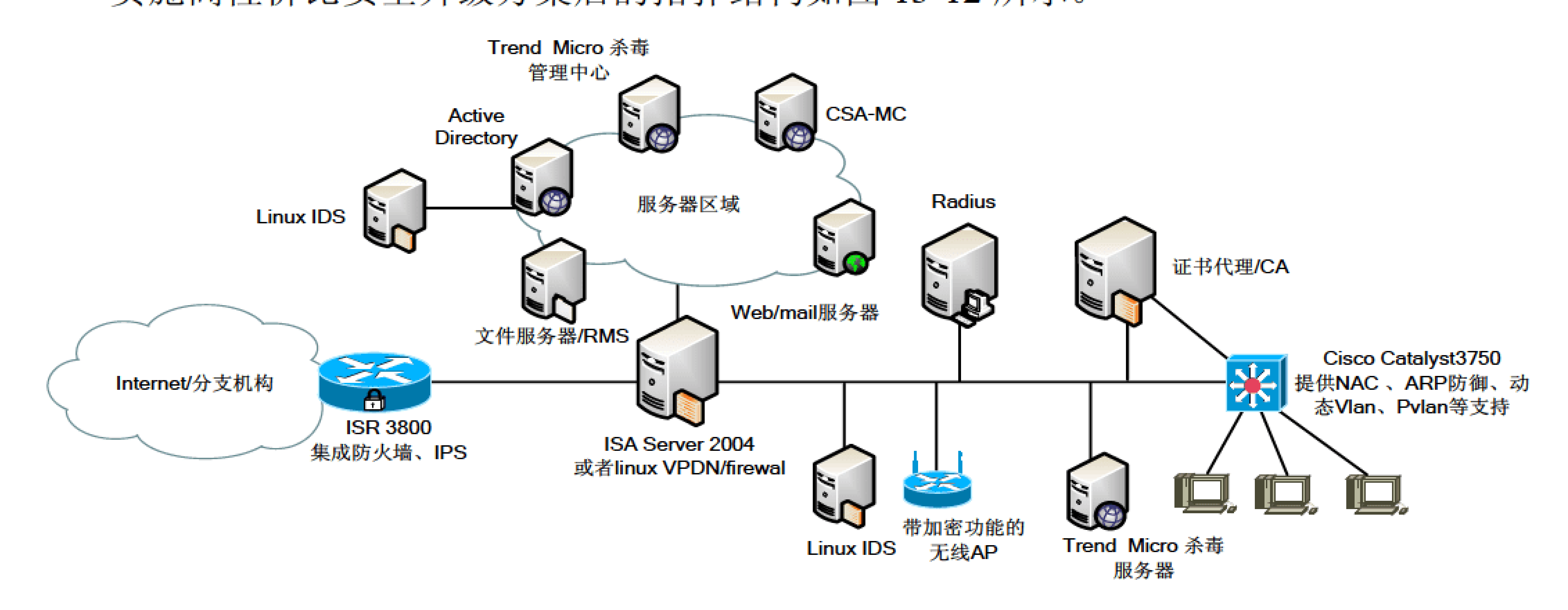


图 13-12　中型企业总部网络高性价比升级方案

3. 高安全性升级方案

在高安全性升级方案中，建议部署 NAC Appliance 的安全接入方案，对于核心网络和边界防火墙进行冗余配置，确保整体安全性能提高。根据实际的情况选择 ASA5510～ASA5550 部署在网络前端，实现统一威胁管理。

建议在 ASA 中使用 CSC-SSM 防病毒网关，同时添置外置的 IPS 4200 系列入侵防御系统组成一个完善的企业网络。将核心网络升级到 Cisco 4500 或使用 3750 堆叠技术完成大量的用户端口访问。使用双机热备份的方式，确保网络安全、稳定。

对于分支机构，可以仍然采用 ASA5005，当然对于规模较大的分支机构也可以采用基于 ASA5510 的平台完成安全保护。

中型企业分支机构网络高安全性升级方案所需设备清单如表 13-8 所示。

表 13-8　中型企业分支机构网络高安全性升级方案设备清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 1841	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Norton/Trend Micro 企业版杀毒软件	1
客户端安全	CSA	为每台电脑配置
	CSA-MC	1
NAC	NAC Clean Access	1
UTM	ASA 5005　或 ASA 5510	视办公区域规模而定

实施高安全性升级后的拓扑结构如图 13-13 所示。

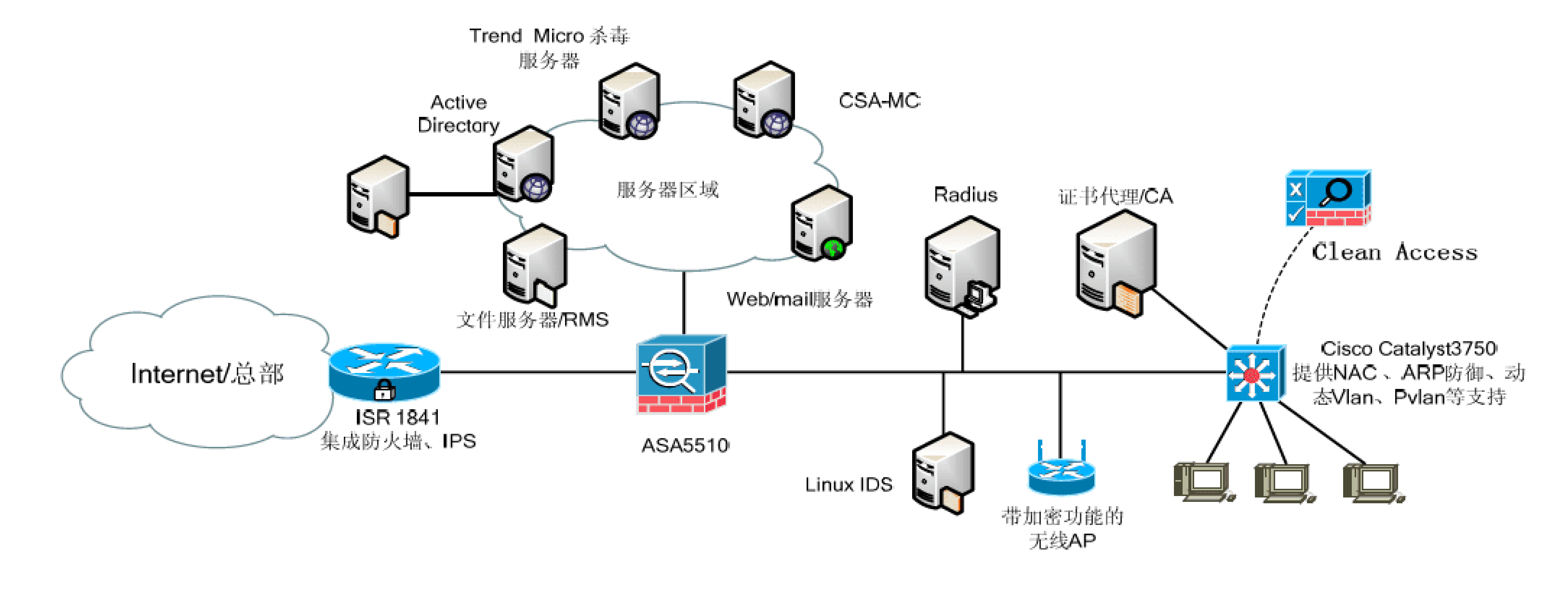


图 13-13　中型企业分支机构网络高安全性升级方案

中型企业总部网络高安全性升级方案所需设备清单如表 13-9 所示。

表 13-9 中型企业总部网络高安全性升级方案设备配置清单

名 称	描 述	数 量
服务器	WSUS 服务器(根服务器)	1
	CA 服务器(根服务器)	2 双机热备份
	AD 服务器(根服务器)	2 双机热备份
	RMS 服务器(根服务器)	1
	Linux 防火墙	1
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 3800	2 双机热备份
	集成 IPS 入侵防御模块	2 双机热备份
交换机	Cisco Catalyst 3750/3560	视端口需求而定
	Cisco Catalyst 4500	2 双机热备份
杀毒软件	Trend Micro 管理中心	1
	Trend Micro 企业版杀毒软件	
IPS	Cisco IPS 4200	视需要监控的区域而定
UTM	ASA 5510～5550	2 双机热备份
	CSC-SSM 内容安全模块	2
NAC	NAC Clean Access Manager(CAM)	1
	NAC Clean Access	1
	Clean Access	每台电脑配置
客户端安全	CSA	每台电脑配置
	CSA-MC	1

实施高安全性升级后的拓扑结构如图 13-14 所示。

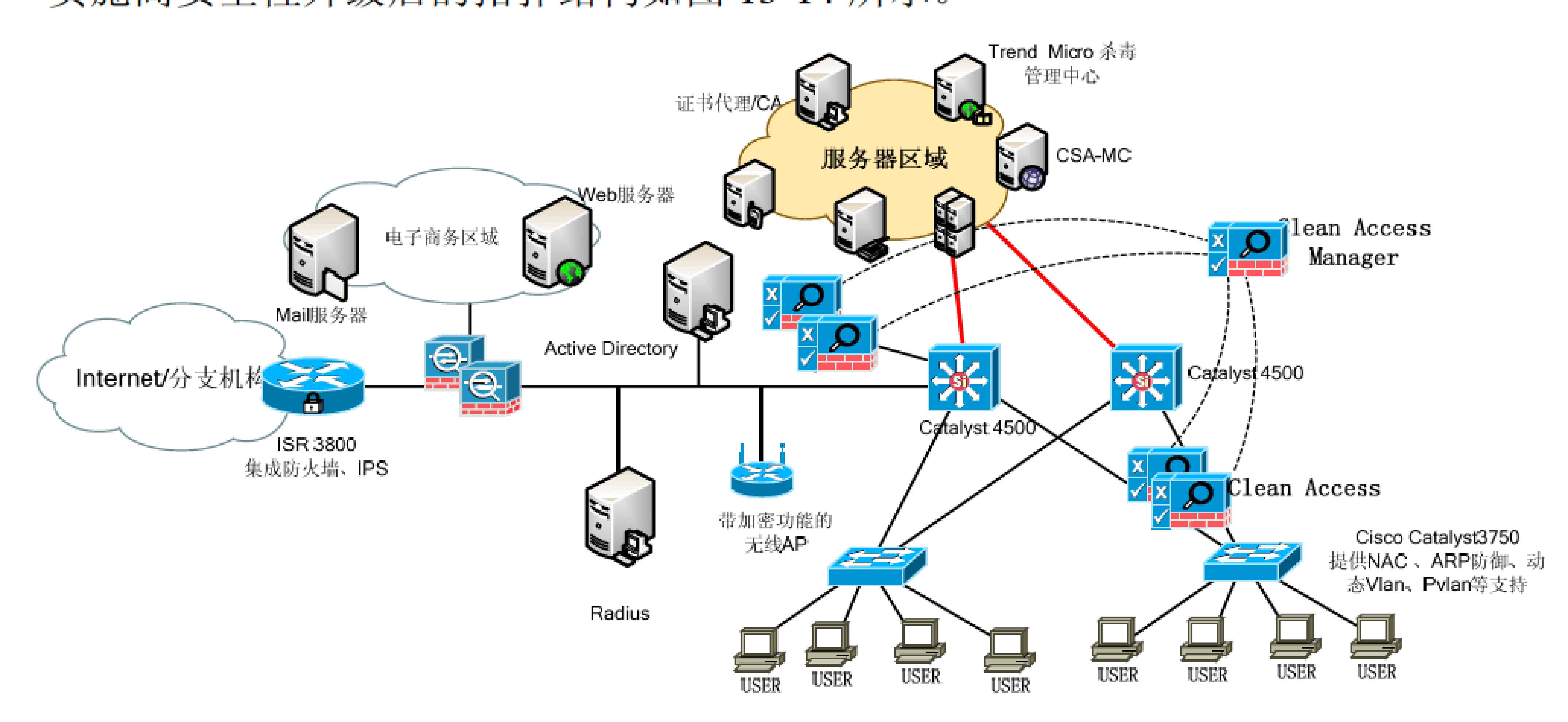


图 13-14 中型企业总部网络高安全性升级方案

13.3 大型企业网络安全设计

应用实例导航：SADNESS 公司网络安全解决方案

※场景呈现

SADNESS 公司是一个在化工行业处于垄断地位的大型企业，在全球拥有众多的分支机构，通常采用网络进行产品销售，电子商务化程度很高；同时该企业无纸化办公程度很高，因此对于网络安全的需求也很高。在公司的发展过程中，由于网络安全问题导致了许多损失，公司非常重视网络安全方面的建设，并愿意对网络安全进行大量的投资。SADNESS 公司的网络拓扑结构如图 13-15 所示。

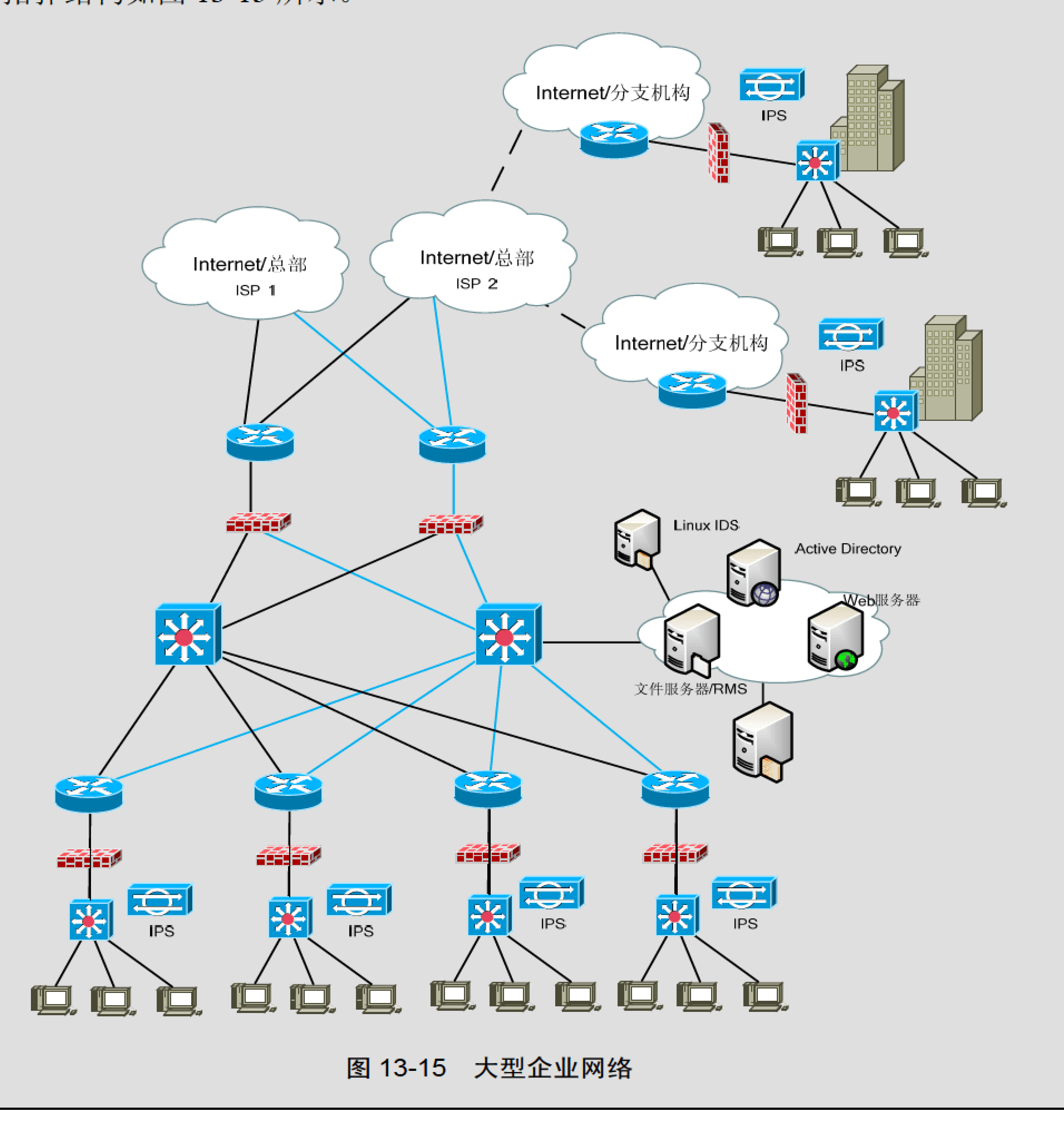


图 13-15 大型企业网络

为了保证网络安全，SADNESS 公司每个部门和每个分支机构都配备了防火墙和 IPS 系统，并安装了大量的杀毒软件。由于分支机构经常软件升级不及时等情况，导致分支机构成为傀儡网络，对公司总部骨干网络发起 DDoS 攻击等。

对于如 SADNESS 公司这类企业，我们通常需要从全局进行考虑整个网络的安全性，并对网络安全设备进行集中管理；同时，还需要考虑使用一个设备虚拟成多个设备进行部署，降低网络受到攻击时的系统风险。

建议公司总部配置 Trend Micro 企业级防病毒系统，配置 NAC Appliance；由于有大量的设备和管理员，必须配置 AAA 管理服务器；建议安装 Cisco Works 进行网络管理，使用 CS-MARS 对企业内部的所有安全设备进行监控；为了节约成本和使用集中的管理方式，建议核心交换机使用 Cisco 6500 系列，并部署集成 IDSM-2 和 FWSM 的模块，以提供集中的防火墙和入侵检测分析功能，如图 13-16 所示。

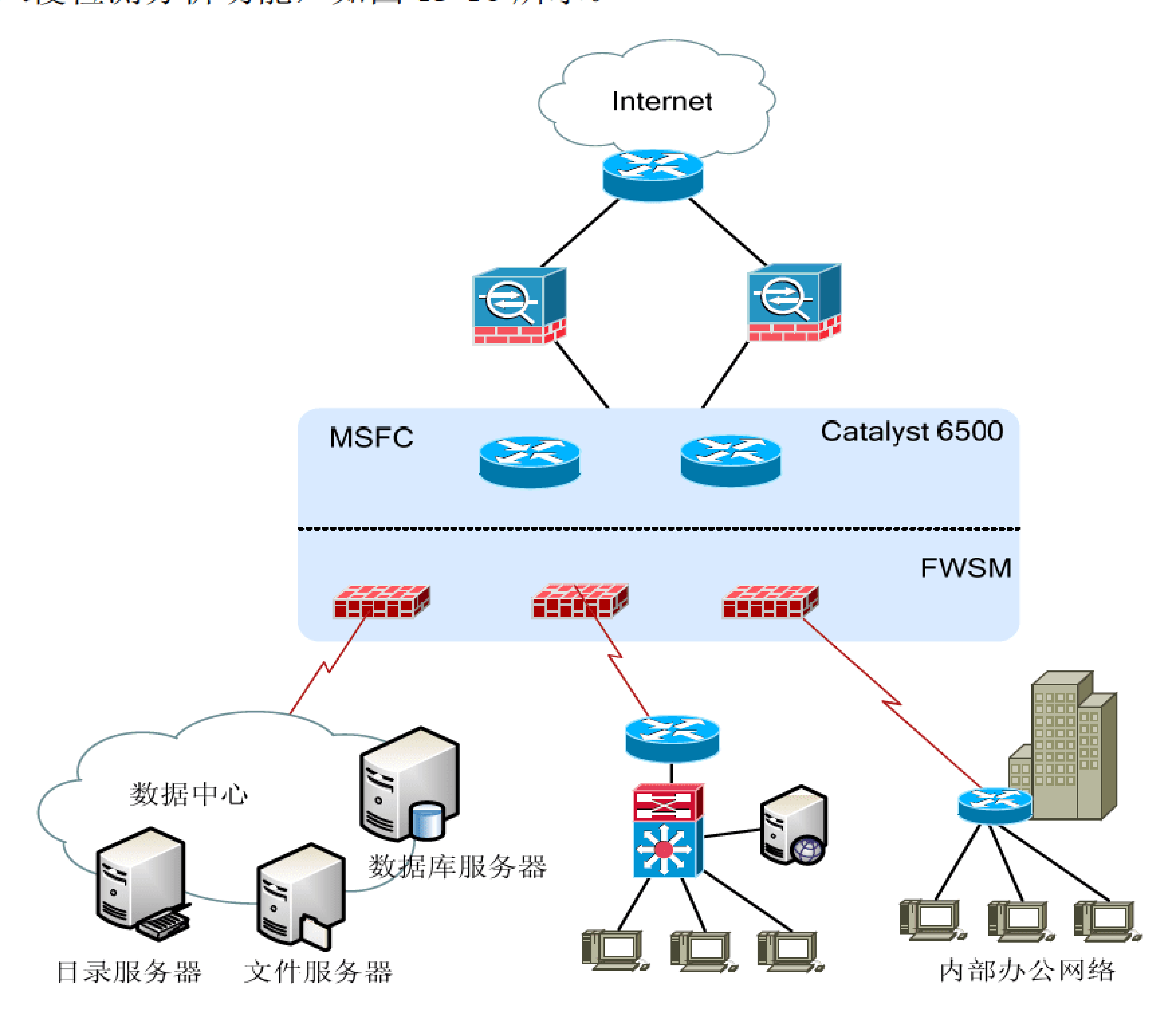


图 13-16 大型企业网络拓扑结构

建议使用 WSUS 自动升级服务器为网络服务器和客户机提供升级服务，使用 Cisco ICS 对网络设备进行升级；为防御 DDoS 攻击，建议部署 DDoS 防御系统。

我们还建议这类用户在其企业网络中为关键的设备配置足够的冗余空间，并且对于数据中心建议使用异地数据备份的方式。

整个大型企业网络所需服务器、硬件环境及安全设备如图 13-17 所示。

实施大型企业总部网络安全性升级方案所需设备清单如表 13-10 所示。

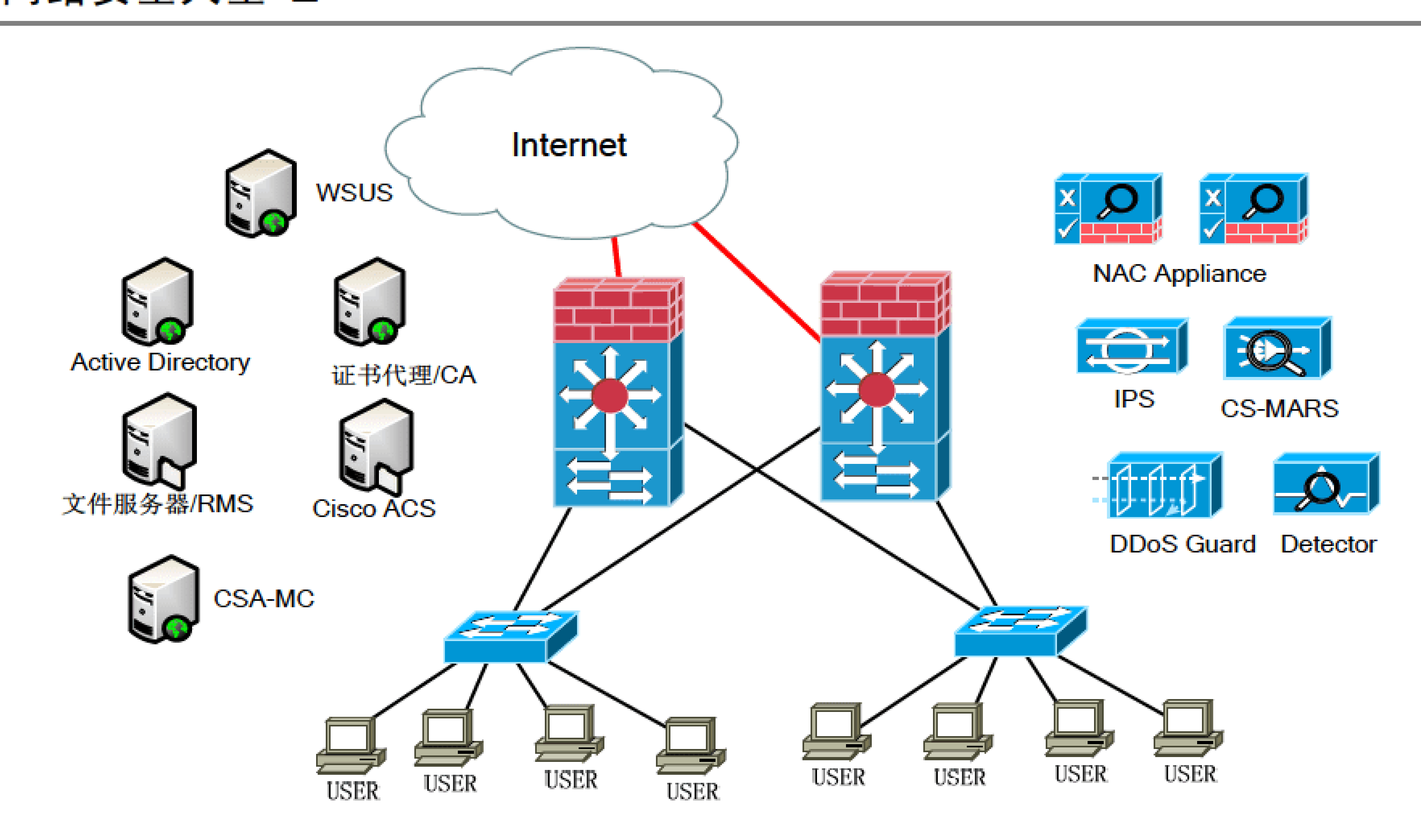


图 13-17 大型企业网络所需要的服务器、硬件环境及安全设备

表 13-10 大型企业总部网络安全性升级方案设备清单

名 称	描 述	数 量
服务器	WSUS 服务器(根服务器)	多台分布式部署
	CA 服务器(根服务器)	2 双机热备份
	AD 服务器(根服务器)	2 双机热备份
	RMS 服务器(根服务器)	1
	Linux 防火墙	1
	Cisco Secure ACS 服务器	2
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 3800	2 双机热备份
	集成 IPS 入侵防御模块	2 双机热备份
交换机	Cisco Catalyst 3750/3560	视端口需求而定
	Cisco Catalyst 6500	2 双机热备份
杀毒软件	Trend Micro 管理中心	1
	Trend Micro 企业版杀毒软件	
UTM	ASA 5510～5550	2 双机热备份
	CSC-SSM 内容安全模块	2
NAC	NAC Clean Access Manager(CAM)	1
	NAC Clean Access	1
	Clean Access	每台电脑配置
客户端安全	CSA	每台电脑配置
	CSA-MC	1
入侵检测	ISDM-2	视需要监控的端口数量而定
	IPS 4200	用于部署在边界
DDoS	DDos Guard XT	2
	DDoS Guard Detector	2

续表

名　称	描　述	数　量
安全响应	CS-MARS Global	1
	CS-MARS Local	每个分支机构配置一台
流量管理	Cisco SCE 2000	2
快速响应	Cisco ICS 服务器	1

实施大型企业分支机构网络安全性升级方案所需设备清单如表 13-11 所示。

表 13-11　大型企业分支机构网络安全性升级方案设置清单

名　称	描　述	数　量
服务器	WSUS 服务器	1
	CA 服务器	1
	AD 服务器	1
	RMS 服务器	1
	Linux 防火墙	1
	Linux Snort IDS	2
	Cisco Secure ACS 服务器	1
无线网	提供加密接入的无线路由器或无线 AP	视办公区域规模而定
路由器	Cisco ISR 1841	1
	集成 IPS 入侵防御模块	1
交换机	Cisco Catalyst 3750/3560	1
杀毒软件	Norton/Trend Micro　企业版杀毒软件	1
客户端安全	CSA	为每台电脑配置
	CSA-MC	1
NAC	NAC Clean Access	1
UTM	ASA 5005　或 ASA 5510	视办公区域规模而定
安全响应	CS-MARS Local	1

实施网络安全性升级后的拓扑结构如图 13-18 所示。

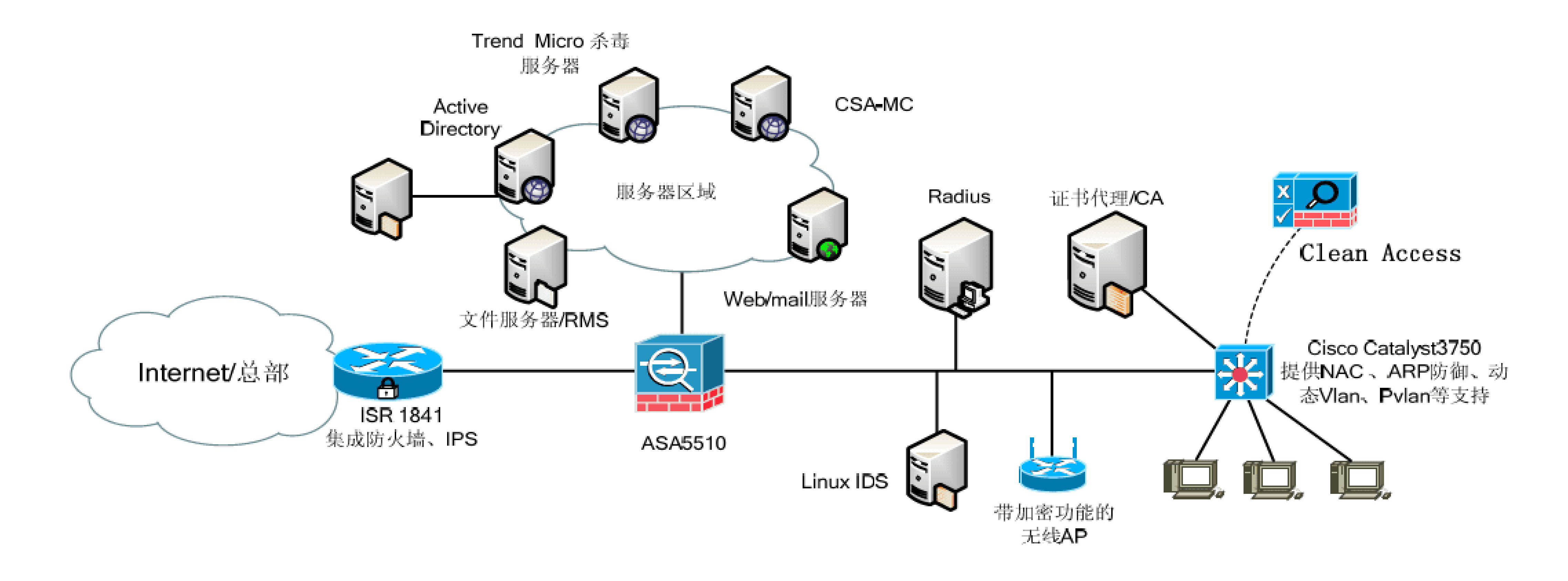


图 13-18　大型企业分支机构网络安全性升级方案

13.4 校园网络安全设计

应用实例导航：AST 大学校园网络安全解决方案

※场景呈现

AST 大学属于全国重点高校，随着校园信息化建设，校园网络中接入的设备越来越多。由于经费问题，没有及时对网络进行升级，网络设备采购没有持续性，每一笔采购都采用不同厂商的产品，导致网络管理难度较大。由于以太网部署方式，导致校园网内的病毒泛滥。

随着学校的发展，学校逐渐实施一卡通项目，整个网络的安全性将变得更加重要。如果出现网络攻击导致一卡通系统故障，将会给全校师生的生活带来非常大的不便，并产生大量的经济损失。

AST 大学由老校区和若干个分校区组成，其拓扑结构如图 13-19 所示。

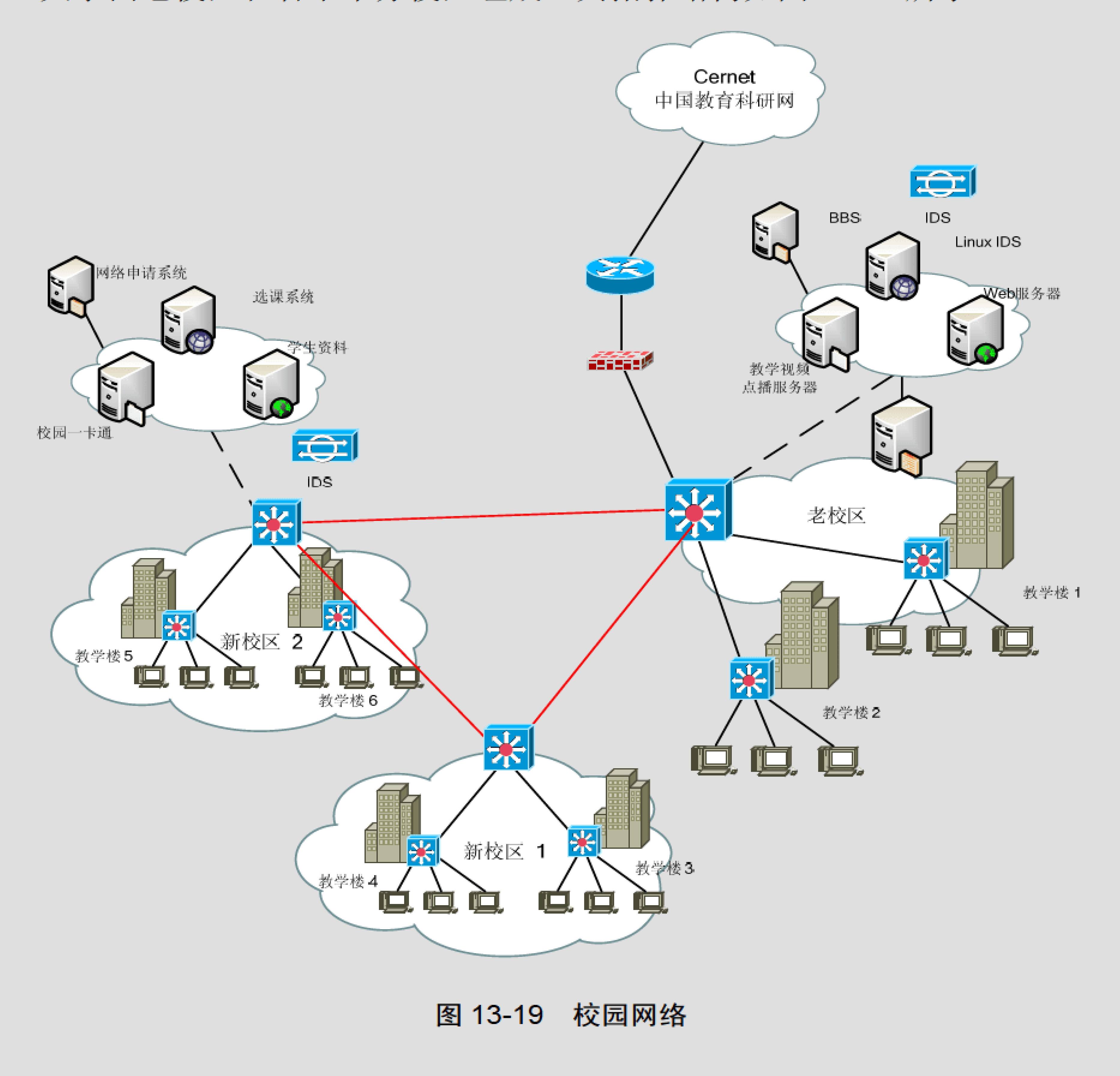


图 13-19 校园网络

近几年的扩招，导致 AST 大学没有足够的财力用于网络安全方面的建设。目前，AST 大学使用该校信息安全学院自己研发的一些安全设备来提升网络的安全性，例如基于 Linux 的防火墙、内容过滤、IDS 等系统。除此之外，还采用一些免费软件用于网络安全监控等。

建设一个安全可靠、稳定可管理的网络已成为人们的共识。对校园网而言，这可能需要管理者们付出更大的努力。高校校园网服务于教学科研的宗旨，决定了其必然是一个管理相对宽松的开放式系统，无法做到像企业网一样进行严格统一的管理，这使得保障校园网安全成为一个大的挑战。对于应用实例导航所提及的 AST 大学，如何选择相对廉价的网络安全产品并有效地提高网络安全性成为安全升级的重点。

对于校园网络安全，AST 大学的案例值得我们学习和借鉴。下面简要地介绍该校在网络安全采取的技术和管理措施，这些措施可能不是很全面很系统，但对校园网的管理人员最少起到一个抛砖引玉的作用。

(1) 部署基于 Cisco Catalyst 6500 的核心设备，并集成 FWSM 和 IDSM-2 来实现集中的安全管理功能。对于接入用户，可以采用 PPPoE 的方式进行接入认证。

(2) 从自身情况出发，根据不同控制策略的要求，对校园网边界路由器、各校区核心交换机、汇聚点交换机以及楼内三层交换机分级配置合理的访问控制列表(ACL)，从而保障网络安全。相关配置机制如下。

- ✧ 对蠕虫病毒常见传播端口和其他特征的控制，可以有效控制蠕虫病毒大面积扩散。
- ✧ 对常见木马端口和系统漏洞开放端口的控制，可以有效降低网络攻击和扫描的成功率。
- ✧ 对 IP 源地址的检查将使部分攻击者无法冒用合法用户的 IP 地址发动攻击。
- ✧ 对部分 ICMP 报文的控制将有助于降低 Smurf 攻击的威胁。
- ✧ 在网络安全日常管理维护和出现病毒爆发或其他突发安全威胁时，合理配置 ACL 将有助于快速定位和清除威胁。

(3) 校园网采用用户静态 IP 地址管理模式。所有网络用户入网前需要事先从网络中心申请获取静态 IP 地址。网络中心收到申请后在用户接入的二层交换机上完成一次用户 MAC 与接入交换机端口的绑定，并在用户楼内三层交换机上实现用户 IP/MAC 绑定，使用这种方法来确认最终用户，消除 IP 地址盗用等情况。虽然看上去比较复杂，但由于网络中心针对校园网中使用的各种不同厂家和类型交换机都开发了相应的绑定程序，所有的绑定管理工作都由程序自动完成，所以管理人员的工作量并不大。网络中心的网管数据库里存放着全校范围内数千台接入交换机的端口-用户房间端口信息数据，以及所有用户的详细使用信息和相关 IP-MAC 资料，所有这些都为建立可管理的安全校园网提供了基础。这种管理模式的好处很多：一旦出现扫描攻击、垃圾邮件等网络安全事件，根据 IP/MAC/端口可以在第一时间迅速定位来源，从而为采取下一步处理措施提供准确的依据。这样一个完整准确的用户信息系统，为以后构想中的网络自防御体系创造了条件。

(4) 在病毒的防控方面，学校采取中央集中控制管理的模式，统一采购网络版杀毒软件，免费提供给校内用户使用，使得病毒库可以及时快速升级。此外，建立一个校内网络安全站点及时发布安全公告，提供一些安全建议和相关安全工具下载也是十分必要的。

(5) 在 2003 年冲击波病毒爆发以后，网络中心开始思考如何应对由于微软操作系统漏

洞引起的大规模蠕虫病毒感染。当年就建立了微软软件更新(SUS)站点，给校园网用户提供微软操作系统补丁的快速自动更新。今年又建立了微软 Windows 软件更新(WSUS)站点和 Linux 系列操作系统的自动更新站点，提供操作系统、微软 Office 应用程序、SQL 数据库的校内快速自动更新服务。因为 WSUS 的数据库里可以存储所有用户的更新信息，所以网络中心就可以掌握校内计算机的漏洞分布情况，并且用户是否安装了补丁可以一目了然。为了普及校内计算机安装自动更新，尽可能消除操作系统级别的安全隐患，进行半强制性的安装。

(6) 在校园网边界出口部署了 IDS，在核心路由器上启用了 NetFlow、sFlow 等进行监控，对关键的网络结点通过端口镜像、分光等方式进行进一步分析处理网络数据包，通过部署基于 Nessus 的漏洞扫描服务器对校园网计算机进行定期安全扫描。及时查看并分析处理这些监控数据和报表有助于在第一时间发现异常网络安全事件并进行处理，防患于未然。

(7) 对于无线网络的安全而言，用户接入认证是非常关键的。网络中心使用了校内统一身份认证来限制校外用户未经授权的无线访问。由于 WEP 认证具有天然的弱安全性，网络中心又同时提供了基于 802.1x 的认证平台进行校内统一身份认证并鼓励用户使用。

(8) 宿舍网的网络安全管理在很多学校往往是比较头疼的，AST 大学网络中心在这方面取得了让学校师生满意的效果，而且，网络中心也没有太多人力投入其中。根本原因还是在学校有关部门的大力配合下，建立了一支由数百人组成的学生宿舍网管员队伍，每座楼都配有至少一名学生网管员，一般在楼内招聘。日常管理由学生工作部门负责，工资待遇纳入学校勤工助学体系，网管员的具体工作由网络中心加以指导。 通过培训这些学生网管员掌握基本的网络安全意识和技能，大量的网络安全问题都消失在萌芽状态。当处于病毒爆发期或有网络安全突发事件时，分布在全校各处的学生网管员也可以第一时间作出响应，协助网络中心的工作。

13.5 运营商网络安全设计

运营商网络需要保护的设备主要是路由器、交换机等数据转发设备的安全、IDC 中的服务器安全以及全网的攻击防范，特别是 DDoS 攻击和蠕虫病毒。对这两种可能对互联网造成大范围网络瘫痪和巨大经济损失的网络安全事故，运营商需要采用一切必要技术和管理手段进行防范。因此我们建议使用基于 Arbor PeakFlow 进行流量分析，并建立 DDoS 清洗中心进行防御。同时，通过 Cisco Works、CS-MARS(CS-MARS 可以配置为 Global 模式和 Local 模式，从而实现 Cluster 的部署方式)、ICS 等系统的部署，可以方便地对系统进行安全管理，如图 13-20 所示。

通常，运营商网络中的大多数病毒来自宽带接入用户，因此有必要使用 MPLS 等方式对宽带接入用户和企业用户进行分离。同时运营商可以部署基于 Cisco CRS-1 的数据交换平台，即便是在严重的 DoS 或者 DDoS 攻击导致线卡超出 CRS-1 的插槽容量时，控制机制会以特定用途集成电路(ASIC)的速度执行，将超出线卡容量的分组导入第三层模块化服务卡(MSC)上的硅分组处理器，从而确保控制面板分组得到优先处理。在网络管理员利用其他安全工具安装缓解方案以解决问题时，这种功能可以保持拓扑的完整性。

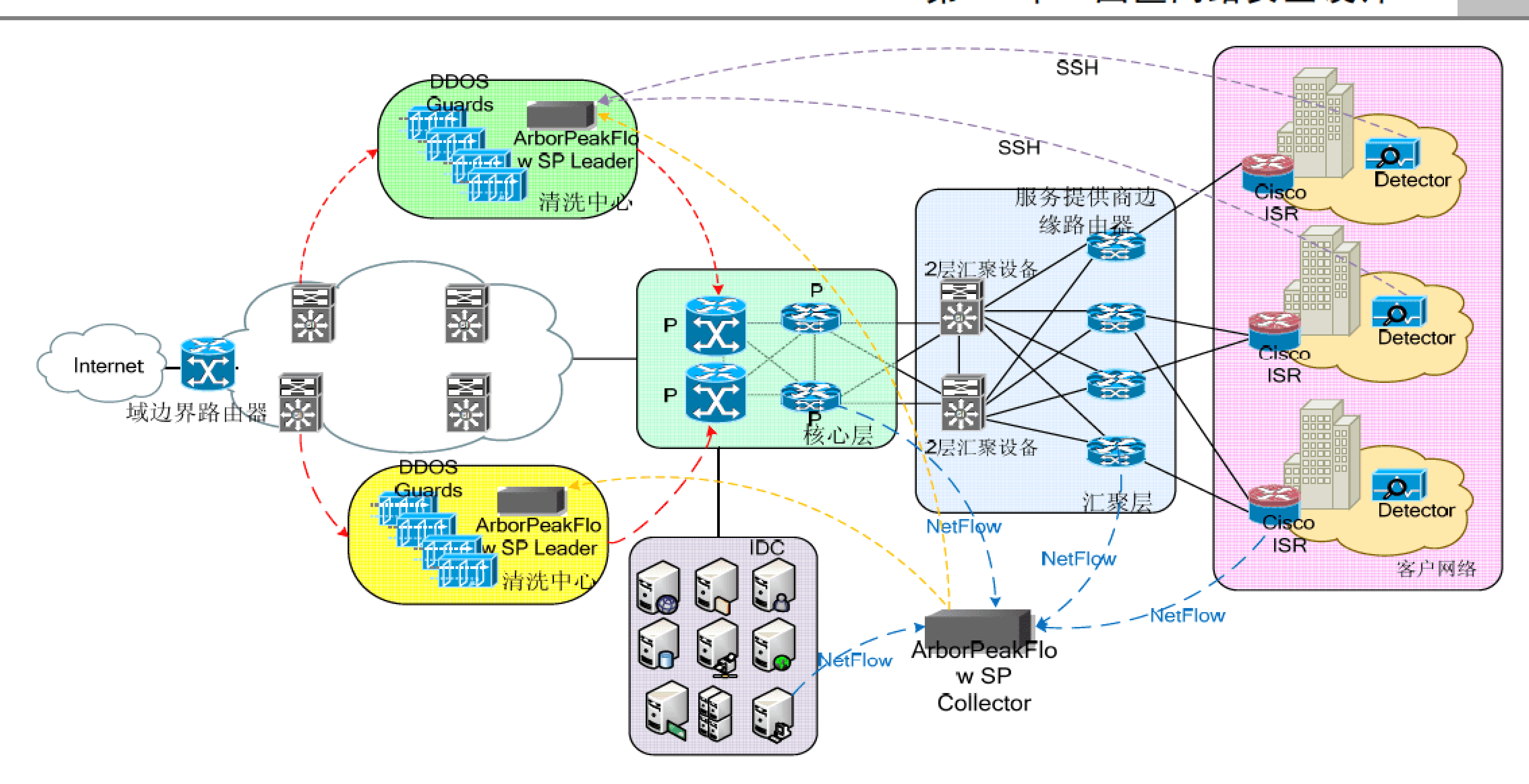


图 13-20　运营商 DDoS 蠕虫清洗系统

对于运营商网络，还需要保证如下协议的安全。

✧ 通过路由协议认证的方式保证 ISIS、BGP 路由协议安全。
✧ 限制用户 VRF 表的大小，保证 MPLS 网络安全。
✧ 对 PIM 协议进行 MD5 认证、对 MSDP 进行 MD5 认证，保证组播网络安全，防止利用虚假 SA 消息对 MSDP 进行 DDoS 攻击。
✧ 保护 NTP Server，防止因为时间混乱导致计费不准等事故。
✧ 保护 VTY 线路，防止黑客登录。
✧ 关闭网络设备 HTTP 等不用的访问，同时保护 SNMP 安全。
✧ 设备访问采用 AAA 集中认证。
✧ 开启设备 NetFlow、sFlow 等流量检测，对于 10G 链路采用 1∶4000 采样、2.5G 以下链路采用 1∶1000 采样。
✧ 对 IGP、BGP 路由协议汇聚参数进行分析，并使用被动侦听的方式检测路由震荡信息。

13.6　本 章 小 结

本章介绍了各种类型网络的安全部署方式，企业、学校、运营商可以根据自身的实际需求进行分析并部署网络安全设备。但是需要牢记的是，网络安全永远是一个整体，网络安全性能的高低取决于最薄弱的一个设备。因此指定网络安全升级方案是需要全局统筹进行。对于企业发展而言，设备购买也需要有持续性，尽量选择一个厂商的设备，并实行统一安全管理。

参 考 文 献

1. 配置 Windows 2003 EFS, http://tech.163.com/06/0626/19/2KIL443400091VCV.html
2. 深入剖析 EFS, http://www.xfocus.net/articles/200506/803.html
3. Enrolling for Certificates from a Cisco Router, http://www.tburke.net/info/reskittools/topics/mscep_enrolling.html
4. John D. Hardin.Linux VPN Masquerade HOWTO, http://www.tldp.org/HOWTO/VPN-Masquerade-HOWTO.html
5. 构建小型的入侵检测系统, http://www.haoxiai.net/caozuoxitong/freebsd/89197.html
6. Snort(入侵检测系统)中文手册, http://bbs.54master.com/223595,1,1
7. Oskar Andreasson.Iptables 指南 1.1.19, http://iptables-tutorial.frozentux.net/cn/iptables-tutorial-cn-1.1.19.html
8. Vijay Bollapragada, Mohamed Khalid, Scott Wainner. IPSec VPN Design. San Jose, California: Cisco Press, 2005
9. Dave Hucaby. Cisco ASA and PIX Firewall Handbook. San Jose, California: Cisco Press, 2005
10. Saadat Malik. Network Security Principles and Practices. San Jose, California: Cisco Press, 2002
11. Dale Tesch, Greg Abelar. Security Threat Mitigation and Response: Understanding Cisco Security MARS. San Jose, California: Cisco Press, 2006
12. Chad Sullivan, Jeff Asher, Paul Mauvais. Advanced Host Intrusion Prevention with CSA. San Jose, California: Cisco Press, 2006

参 考 资 料

1. 配置 Windows 2003 EFS,http://tech.163.com/06/0626/19/2KIL443400091VCV.html
2. 深入剖析 EFS , http://www.xfocus.net/articles/200506/803.html
3. Enrolling for Certificates from a Cisco Router http://www.tburke.net/info/reskittools/topics/mscep_enrolling.htm
4. Linux VPN Masquerade HOWTO
5. IPSec VPN 与 SSL VPN 优劣比较 http://cisco.chinaitlab.com/vpn/25116.html
6. 构建小型的入侵检测系统
7. Snort(入侵检测系统)中文手册
8. Iptables 指南 1.1.19
9. 下一代网络安全，思科系统(中国)网络技术有限公司
10. Cisco.Press.IPSec VPN Design(2005)
11. Cisco.Press.Advanced.Host.Intrusion.Prevention.with.CSA.
12. Cisco.Press.CCIE.Self.Study.CCIE.Security.Exam.Certification.Guide
13. Cisco.Press.CCIE.Self.Study.CCIE.Security.Practice.Labs
14. Cisco.Press.CCSP.Cisco.Secure.PIX.Firewall.Advanced.Exam.Certification.Guide.2nd.Edition.
15. Cisco.Press.CCSP.CSI.Exam.Certification.Guide.2nd.Edition.
16. Cisco.Press.CCSP.IPS.Exam.Certification.Guide.
17. Cisco.Press.CCSP.SNPA.Official.Exam.Certification.Guide.3rd.Edition
18. Cisco.Press.CCSP.SNRS.Exam.Certification.Guide.2nd.Edition.
19. Cisco.Press.Cisco.Access.Control.Security.AAA.Administration.Services.May
20. Cisco.Press.Cisco.ASA.All-in-One.Firewall.IPS.and.VPN.Adaptive.Security.Appliance
21. Cisco.Press.Cisco.ASA.and.PIX.Firewall.Handbook.
22. Cisco.Press.Cisco.Security.Agent.
23. Cisco.Press.Firewall.Fundamentals
24. Cisco.Press.Network.Security.Principles.and.Practices
25. Cisco.Press.Network.Security.Fundamentals.
26. Cisco.Press.Network.Security.Architectures.
27. Cisco.Press.Security Threat Mitigation and Response: Understanding Cisco Security MARS
28. Cisco.Press.Self.Defending.Networks.The.Next.Generation.of.Network.Security.
29. Cisco.Press.The Complete Cisco VPN Configuration Guide(2005)
30. Cisco.Press.WLAN Security
31. Cisco.Press.Securing.Your.Business.with.Cisco.ASA.and.PIX.Firewalls.
32. Cisco.Press.Designing.VPN.Security
33. Cisco.Press.IPsec.Virtual.Private.Network.Fundamentals
34. Cisco.Press.Cisco.Router.Firewall.Security.
35. Cisco.Press.Cisco.NAC.Appliance